A. The primary functionality did not change. There were variations and additional --
Q. Doctor, it changed over time.
A. It did change, yes.
Q. And, in fact, there was a second demonstration of DVPN; isn't that right?
A. I believe that's correct.
Q. I think it was in March of 2000?
A. That sounds correct.
Q. So that's -- March of 2000 is at least a month before the '180 patent was filed, right?
A. That's correct, yes.
Q. But you haven't offered any opinions that the DVPN technology from that meeting invalidates any claim of any VirnetX patents; isn't that right?
A. That's correct. I focused on the earlier demonstration.
Q. And that's because the later demonstration doesn't invalidate any claim of the VirnetX patents; isn't that right?
A. I don't know.
Q. Your attorney has not asked you to look at that one?
A. I didn't look at it, and I don't believe anyone asked me to.

Q. Now, back to the source code, we talked about how there were multiple codes in this case, right?
A. That's right.
Q. There was a Defendant's 3353?
A. I can't see it.
Q. Take my word for it. It's some source code. Defendant's Exhibit 3062, some more source code.
A. Okay.
Q. Can't really see it. I think there were multiple versions of the DVPN code on this one.
You looked at all of this code, right?
A. Yes, I did.
Q. And it had different dates?
A. That's correct.
Q. Some from 1998; some from '99; some from 2000; some from '97?
A. Exactly.
Q. All right. But then you chose Defendant's Exhibit 3061. That's the one you relied on, right?
A. That sounds correct, yes.
Q. You relied on your attorney's guidance. They're the ones that helped you identify the right source code to look at, right?
A. I did look at all the source code. I did have some guidance as to which was older and which was

younger, et cetera.

Q. Your attorneys helped you identify Defendant's Exhibit 3061 to look at; isn't that right?

A. Again, no. They provided me with all the source code.

Q. They told you to look at this one for your opinions in this case, didn't they?

A. I don't recall that being the case.

Q. Look at your deposition.

MR. McLEROY: Would you pull up Page 249 of your deposition?

THE WITNESS: Do I have that in front of me?

MR. McLEROY: Oh, I don't think I've given it to you yet.

THE WITNESS: Thank you.

MR. McLEROY: If you could, Mr. Moreno, blow up the portion starting at Line 11 of Page 249.

Q. (By Mr. McLeroy) You remember when I took your deposition, Dr. Wicker?

A. Yes, I do.

Q. It was, I think, in New York City, right, when I came up to New York to visit you?

A. Yes, that's right.

Q. It was at your law firm's office there in downtown Manhattan, right?

A. Yes, it was.

Q. And you were under oath then just like you're under oath today?

A. Yes.

Q. And I think the first question in this sequence that I asked you was: Now, was there only one version of the DVPN source code provided?

ANSWER: The one I looked at -- actually, I take that back. I think I saw several. But I did see the one that was associated with the public demonstration.

And I asked you: Well, how were you able to determine that it was associated with the public demonstration?

And your answer was, at that time at least: That would have been through the deposition testimony.

Do you see that?

A. Yes.

Q. And I followed up, skipping down a little bit.

Question: Whose deposition; do you remember?

You said: Actually, I don't. I don't remember specifically.

I said: Well, let me see if I can refresh your recollection. There are two guys, Sterne and

Kindred, from Sparta?

You said: That's right.

I said: Was it one of those two guys?

Your answer was: Frankly, sitting here at this late hour, I can't remember how I knew which version was actually demonstrated. It may have simply been represented to me that that was a fact.

Do you see that?

A. Yes, I do.

Q. And I asked you: Represented to you by the lawyers?

You said: Well, they're not my lawyers, but yes.

And I clarified: By Microsoft's lawyers?

And you said: Yes, that's correct.

Do you see that?

A. Yes, I do.

Q. That testimony is still truthful, right? You were telling the truth at the time?

A. Yes. I didn't know then, and I'm not sure now.

Q. Now, Dr. Wicker, let's assume that you and Microsoft lawyers are correct, and you actually did identify the right version of code that was used at that March 1998 demonstration.

A. Yes.
Q. Without talking to Mr. Turchi, who actually wrote the code, okay, are you absolutely certain that this source code authoritatively describes what was shown at the demonstration?
A. I think that the evidence is clear as to what was shown at the demonstration and the source code --
Q. Dr. Wicker --
A. -- reflects what was at the demonstration.
Q. Dr. Wicker, that's not my question.
Are you certain, with authority, that that source code was the source code used for the demonstration?
A. As certain as I can be.
Q. See what Mr. Sterne said about that when he was asked a similar question.
MR. McLEROY: If we can go to -- I'm sorry -- Slide 23.
Sorry. It's Mr. Kindred's testimony.
Q. (By Mr. McLeroy) He said: And, again, in order to know exactly what was demonstrated in the spring of '98, you'd need to look at the source code. Spring of '98, he was referring to March of 1998; don't you think?
A. Yes, I think that's right.

Q. He said: To know exactly what was demonstrated, yes.
But then he caught himself. You see that?
He said: Let me qualify that. And then he said: That wouldn't be authoritative either, because the demonstration didn't show everything that was in the implementation.
Do you see that?
A. Yeah. Yes, I see that.
Q. We didn't get to ask Mr. Turchi that question, did we?
A. No, not as far as I know.
Q. Now, a few more questions about DVPN.
MR. McLEROY: Your Honor, do you mind if I approach the demonstration board again?
THE COURT: You may.
MR. McLEROY: I appreciate the help.
Q. (By Mr. McLeroy) Unfortunately, Dr. Wicker, it looks like your markers are fading.
A. Yes, I noticed that.
Q. Invisible ink makes it harder to cross-examine, huh?
Secure DNS request, that's what you wrote there, right?
A. That's right.

Q. That's probably hard for the jury to see now.
And you showed it going from the Red Cross client to Red Cross firewall; is that right?
A. That's correct.
Q. It was that request -- that was the first thing you drew on the board, right?
A. I believe it was, yes.
Q. So that's what triggered the setting up of the VPN; that right?
A. Well, there were a number of steps in between, but, yes, that was the first step to what eventually caused that VPN between the two firewalls to be created.
Q. Dr. Wicker, that was the first step, right?
A. Yeah.
Q. That was the trigger?
A. It was the first step.
Q. It was the trigger?
A. The trigger is the determination step that's caused when the Red Cross firewall goes to the coalition manager and finds that there's a secure association --
Q. So it's your testimony that trigger means determination? Yes or no, trigger means determination?
A. Well, that's what -- well, I should ask you what you meant by trigger, so I can give you a good answer to your question.

To me, I thought -- when you said trigger, I thought that you were referring to the step that caused the establishment of VPN.

Q. A trigger means first step, okay?

A. Okay.

Q. You say it's the DNS request the triggers this process, right?

A. Well, if that's the first step --

Q. Take the definition we just agreed on.

A. I'm sorry?

Q. If you take the definition we just agreed on, the trigger being the first step, you agree that the DNS request triggers this process?

A. The DNS request is the first step.

Q. That's your testimony?

MR. McLEROY: Could you go Slide 24 now?

Q. (By Mr. McLeroy) This is what Mr. Saydjari said in his deposition, and he was confronted with his testimony yesterday.

Do you remember when he talked about that with Mr. Cawley?

A. Yes, I do. Or I should say I read the transcript. I actually wasn't in court. I saw it.

Q. He said: I would doubt that they would use the DNS call to trigger.

Do you remember that?
A. Yes.
Q. Now, Mr. Saydjari actually attended this meeting, didn't he?
A. Yes, that's correct.
Q. He was there; he has firsthand knowledge?
A. I believe that's what he said, yes.
Q. And he was paid by Microsoft to travel down to Tyler and participate in this lawsuit, right?
A. Yes, they paid for his time.
Q. And his testimony was that I doubt they would use the DNS call to trigger.
See that?
A. Yes.
Q. All right. Dr. Wicker, let's move on to Aventail. We're running out of time. I'll just cover a quick point with you.
MR. McLEROY: Your Honor, do you mind if I switch out to the Aventail board?
THE COURT: No. You may.
MR. McLEROY: Now I know why you were handling these over there.
Q. (By Mr. McLeroy) You identified the client computer and the Aventail system on this board as the computer on the very far left.

Do you see that?
A. Yes, that's correct.
Q. That's what you labeled it?
MR. McLEROY: Can we put up Slide 18 of Dr. Wicker's presentation? Of Dr. Wicker's presentation, do you have that?
Q. (By Mr. McLeroy) Here -- and you were talking about, I believe, the context of the '135 patent. This was the client here?
A. No. That is a client in some situations.
In this particular claim, in the '180, I showed how the Aventail SOCKS Server could act as a claim.
Q. Okay. So depending on which claim or which patent you're talking about, you changed the label of client computer, didn't you?
A. No. No, I don't think that's fair.
Q. Dr. Wicker, you labeled the client computer as the computer on the far left here; is that right?
A. Yes, I did.
Q. All right. And then if you look at the monitor, that corresponds to the computer on the far left in your slide, right?
A. That's right.
Q. And then you show two servers. They're

labeled Server 1 and Server 2 up on the big board, the big board up top; is that right?

A. Yes, that's right.

Q. And then you have the SOCKS server and the SOCKS server on the board that's here in the courtroom with us, right?

A. Yes, that's correct.

Q. Those correspond to each other; is that right?

A. Yes. Server 1 in this diagram for proxy chaining is the same as Aventail SOCKS Server on the left as we see on the board, that's right.

Q. All right.

MR. McLEROY: And if you can take that blowup down for a second.

Q. (By Mr. McLeroy) Then there's a destination server on the far right, and that corresponds to what you've labeled the secure website here in your drawing; is that right?

A. That's correct.

MR. McLEROY: If you could just keep it right there.

Q. (By Mr. McLeroy) Now, up on your slide you prepared with the highlighting, you said: Performed by a client computer; is that right?

A. That's correct.

Q. And you highlighted the server labeled Server 1; is that right?
A. That's right.
Q. In this drawing, when you were asked what the client computer is, you labeled this computer here, right? You labeled this Aventail client, right?
A. That's labeled as a client. It is a client.
Q. And those aren't the same two computers, are they?
A. They're both acting as clients.
Q. And I think what you wanted to tell me earlier was that depending on the claim or depending on the patent you're talking about, you would identify different things as a client computer; is that right?
A. No. No. What I'm saying is that in some situations, one could act as a client, and at the same time, another could be acting as a client. It's all relative. Client server architecture --
Q. But --
A. -- are relationships.
Q. So in some situations, the computer on the left is the client. And in other situations, it's the second computer from the left that's the client computer.
Is that your analysis in this case?

A. It's more accurate to say that both can act as clients.
Q. Dr. Wicker, you identified different client computers in these two drawings; that's fair, right?
A. That's correct.
Q. And you did the same thing when you were talking about DVPN; isn't that right?
You identified client computers -- different client computers at different times with different claims, right?
A. That's right. DVPN in different computers could act as clients.
Q. So you didn't consistently identify the same computer as a client computer all the way through this prior art, right?
A. No, I wouldn't agree with that.
Q. You wouldn't agree with that?
A. I consistently showed where computers could act as clients throughout.
Q. You consistently identified multiple computers as the client computer; is that right?
A. Multiple computers can act as clients.
Q. And you had multiple computers that you identified as client computers; is that right?
A. That's correct.

Q. And you pointed to different client computers to meet the different elements of the claims; isn't that right?

A. That's true.

Q. All right. I want to talk briefly now about the '180 patent.

One really big issue on the '180 patent is whether the prior art contains secure domain names; is that right?

A. That's correct.

Q. The term that was defined by the Court; is that right?

A. Yes, that's right.

Q. And you never showed the claim construction of secure domain names in your testimony, did you?

A. I actually described it several times. I never actually put it on the screen.

Q. You didn't put it on the board, did you?

A. No, but I explained it to the jury.

Q. Now, secure domain names, that term shows up in every claim of the '180 patent, right?

A. Yes, that's correct.

Q. And so if the jury decides that the prior art does not teach any secure domain names, you'd agree that none of the claims of the '180 patent are anticipated;

is that right?

A. If the jury decides that the prior art I discussed does not reveal or disclose any secure domain names, then --

Q. Then the claims of the '180 patent would be anticipated; is that right?

A. If it shows -- it has to show the capability for secure domain names. If it doesn't show that, then yes.

Q. Okay. Now, you believe that standard domain names, domain names that have been in existence, I think since, you testified, in the mid-'80s, that those can be security domain names.

That's right, isn't it?

A. Well, 1982, but yes.

Q. And you agree with me, I believe, that the prior art in this -- at issue in this case, it only uses standard domain names; is that right?

A. There are domain names that have the standard, fully qualified domain name structure, if that's what you mean.

Q. Well, let's look at your deposition.

MR. McLEROY: Can you put up Page 64 to 65 of his deposition? Page 64, starting at Line 23.

Q. (By Mr. McLeroy) I asked you there --

MR. McLEROY: Would you put up the next two lines of the next page?
That would be great.
Q. (By Mr. McLeroy) Now, are you aware --
MR. McLEROY: Yes, the first five lines.
Q. (By Mr. McLeroy) Question: Now, are you aware of any prior art references that you rely on that use non-standard domain names?
Did I read that right?
A. Yes.
Q. You said: I can't think of an example of a prior art reference on which I relied that uses domain names, other than those defined as standard in the RFCs.
Is that right?
A. That's correct.
Q. That's consistent with what you just said, right?
A. Right. I still can't.
Q. You just believe that these standard domain names can also be secure domain names; is that right?
That's your opinion?
A. That is correct.
Q. And so you believe that secure domain names of the VirnetX patents, that they can overlap with the standard domain names resolved by a conventional domain

name server; is that right?
A. I'm not sure what you mean by overlap. If you could show me the Court's claim construction, I could point out how a standard domain name could satisfy.
Q. I'd rather show you your deposition.
MR. McLEROY: Can we go to Page 88 of his deposition?
I'm sorry. I need to give you a line number. Line 22 and continue over to 89/1. So 88/22 to 89/1.
Yeah, that's right. Lines 22 and then carrying over to the next page, question and answer.
Q. (By Mr. McLeroy) Question: So it's your opinion that the inventors considered, believed that a secure DNS could overlap with a standard DNS.
So you used the term overlap there, right?
A. Yes.
Q. And your answer was: Yes.
A. Yes.
Q. So you will agree with me that it's your opinion that secure domain names can overlap with conventional or standard domain names; is that right?
A. Well, they can occupy the same DNS server, yes.
Q. And a name can be a secure name at the same

time it can be a conventional name; is that right?
A. I don't think at the same time, but at different times, yes.
Q. Okay. There's no -- nothing that precludes a secure domain name just looking at it from also being a conventional domain name; is that right?
A. Well, again, if it requires authorization, according to the Court's claim construction, then it's secure. If it doesn't require authorization, then it's not secure.
The question of whether it requires authorization may have a different answer over the course of time. So a name over the course of time may be secure at one point and not secure at another, if that's what you're asking.
Q. It's your testimony that the prior art only teaches standard domain names, right?
A. As called for in the art of -- yes, the domain names are standard.
Q. And it's your opinion that something that is a standard domain name can't also at the same time be a secure domain name; is that right? They can't overlap?
A. No. No. That's not right.
Q. So they can overlap?
A. What I said was a name can be secure at one

point and not secure at another.

A standard domain name can be secure at one point and not secure at another point in time.

Q. Let me -- let me do this.

MR. McLEROY: Would you put up Slide 31, please?

Q. (By Mr. McLeroy) Sorry. The font is a little small. This is from the deposition of Dr. Johnson.

Do you see that?

A. Yes, I do.

Q. And he was asked a question, and he answered the question: Do you agree that secure domain names of the claims of the '180 patent do not overlap with standard domain names resolved by the conventional DNS?

Do you see that?

A. Yes, I do.

Q. He answered the question yes, right?

A. That's correct.

Q. Dr. Wicker, how do you answer that question?

A. I would have to know what the context of the question was. If the question is asking me whether a given domain name can be secure at one moment and not secure at another, the answer is yes.

If you're asking whether a secure domain name can reside in a DNS with unsecure names, the answer is

clearly yes.
Can you restate the question? I think I've answered it.
Q. Dr. Johnson was able to answer the question, wasn't he?
And I'll tell you, I honestly didn't understand your answer.
A. Okay. So let's --
Q. I mean, can you answer the question yes or no that Dr. Johnson answered yes or no to?
A. Okay. If he -- if the question, as he understood it, is whether the domain name can be both secure and unsecure at the same time, clearly, that doesn't make sense. That can't be the case.
Q. Dr. Wicker, let's -- I guess let's get to the real issue here.
You don't want to disagree with Dr. Johnson's testimony; isn't that right?
A. Dr. Johnson is a very impressive individual. I just don't know what's being meant -- I don't know the context.
Q. Dr. Wicker, you would agree it would look bad if Microsoft's -- well, how many experts does VirnetX have? It's just Dr. Jones, right?
A. I believe you have a damages expert. I don't

know how many other experts.

Q. Let me be clear. Professor Jones is going to testify. He's offered opinions on infringement and validity; is that right?

A. Yes, sir.

Q. Now, Microsoft, on the other hand, hired Dr. Johnson to opine on invalidity and hired you to testify about -- did I mix this up?

Johnson, infringement; Dr. Wicker, invalidity. Sorry about that.

A. Yes, sir.

Q. I mean, you think it's important that the two separate experts Microsoft hired, that they offer consistent opinions, don't you think?

A. Yes.

Q. It would test Microsoft's credibility if it had one expert that answered this question yes, and another expert that answered this question no.

Don't you agree?

A. Yes.

Q. Dr. Wicker, can you answer this question yes like Dr. Johnson did?

A. To the extent he's saying that a standard domain name cannot be a secure name under the Court's claim construction, I don't agree.

Q. You don't agree with Dr. Johnson. He gave his deposition after the Court's claim construction order came out, didn't he?

A. Yes. There may be other context to the question that I'm not seeing.

Q. Dr. Wicker, you and Dr. Johnson have taken inconsistent positions on this issue, haven't you?

A. I don't agree. I don't know the context of the question.

Q. You just answered the question no, right?

A. As I understand it, I would say no.

MR. McLEROY: Pass the witness.

THE COURT: All right. Redirect?

MR. BOBROW: Thank you, Your Honor.

REDIRECT EXAMINATION

BY MR. BOBROW:

Q. Professor Wicker, during the cross-examination, it began some time ago with some questions about the demonstration that Mr. Pall did here in Court.

Do you recall that testimony?

A. Yes, I do.

Q. And do you recall that Mr. McLeroy came over to this board and pointed to the determining step of Claim 1 of the '135 patent?

Do you recall that?

A. Yes, I do.

Q. Then he pointed to some testimony by Mr. Pall about whether or not that determining step was typically met by the demonstration that was conducted.

Do you remember that as well?

A. Yes, I do.

Q. And do you remember saying that you disagreed with the question that Mr. McLeroy was asking you, but then he interrupted you and wouldn't let you explain why you disagreed with the characterization he was making?

Do you remember that?

A. Yes, I do.

Can you please explain now the answer that you wanted to give then, but that Mr. McLeroy wouldn't let you?

A. Yes. I would be happy to.

In the first demonstration, the one that Mr. Pall did, initially he used -- and, again, I can't remember the name of the website, but it was something like trustedwebsite.com or securewebsite.com.

What happened in that situation was the computer went to a phone book, found securewebsite.com, and the phone book indicated that a VPN was to be created. It determined that the secure VPN connection was necessary. It satisfied the step.

The subsequent demonstrations did not demonstrate that step one way or another, because eBay.com -- and this is not a secure website dot-com -- were not in the phone book. It was not a question of not determining. It simply wasn't in the phone book. And so what the system did then is it went on to try different ways to resolve those names. And at one point, it tried to contact the DNS through that VPN.

So it wasn't a matter -- the second two didn't show that that element was not satisfied. It simply showed that Microsoft indeed is very tenacious in trying to create a connection and to resolve those things.

Q. Now, in your testimony earlier, you had said that the NT 4 operating system had been released in 1996 with PPTP and AutoDial.

Do you recall that?

A. Yes, I do.

Q. And do you recall that Mr. McLeroy pointed at some computers and some software and the like dated in the year 2000?

Do you recall that?

A. Yes.

Q. All right. Now, in your opinion, with your computer science background and the work you've done in this case, does that equipment and software from the

year 2000 impact at all the operation of the executable NT 4 operating system from 1996?
A. It does not affect it at all.
Q. Can you please explain why that is?
A. First off, Windows 2000, the sticker that you saw, that's a later operating system. But for Mr. Pall's demonstration, he wasn't using the Windows 2000 operating system. He was using Windows NT 4, the earlier one from four years back.
Secondly, what he was demonstrating was the software. It's hard to find computers that are -- I'm getting hired; the math is harder -- but 16, 17 years old. So they found a computer that was close and installed the old software on it.
So he demonstrated how the software worked, and that software was from 1996. The fact that that computer once held an older -- excuse me -- a newer operating system is irrelevant.
Q. All right. Now, let me shift gears, and I want to ask you another question about the NT 4 system and AutoDial to follow up on a question that you were asked by Mr. McLeroy.
You may recall that you were asked several questions about AutoDial reconnecting.
Do you remember that?

A. Yes.
Q. And do you remember asking several questions of Mr. McLeroy and providing some answers about what reconnect meant in the context of NT 4 and AutoDial and PPTP VPNs?
Do you remember that?
A. Yes, sir.
Q. And you were asked a question and I believe that Mr. McLeroy again came over here to this board for the '135 patent, and what he pointed to was this phrase, automatically initiating the VPN.
Do you remember that line of questions, sir?
A. Yes, I do.
Q. And what you were asked, I believe, was about the very first time -- the very first time that a connection is made, and I think that you said that you didn't know in the demonstration that was done how the connection was made the very first time; is that right?
A. Yes, that's correct.
Q. All right. Now, from the demonstration that you saw and your knowledge of NT 4, do you know how the VPN was initiated the times thereafter?
A. Yes.
Q. Can you please tell us how the VPNs have been initiated for the second time and the third time and the

fourth time and every other time thereafter?
A. They were initiated automatically by AutoDial.
Q. All right. Shifting now from the NT 4 topic to DVPN, if I may, you were asked some questions about the DVPN source code.
Do you recall that?
A. Yes, I do.
Q. First of all, was the DVPN source code the only information that you considered about the DVPN demonstration that occurred in March of 1998?
A. No. No, I relied on a lot of other information.
Q. Can you tell us and remind us, please, what other information you considered about the DVPN demonstration from 1998, March, besides the source code?
A. Sure. One example was a description of -- a presentation that described the demo. I also had a number of e-mails that described it in detail. And I had deposition testimony.
Q. Now, did you believe -- after your review and study of that information, all the information you considered, did you believe that that information was sufficient to show clearly and convincingly what the demonstration showed in March of 1998 sufficient to show that it anticipated the claims at issue in this case?

A. Yes.
Q. Can you please explain why?
A. There was sufficient evidence. And as you will recall, clear and convincing evidence is the burden.
And when I studied that information, I found that that burden was met. All the information pointed to a demonstration that clearly met all of the asserted claims of the patents-in-suit.
Q. Now, I'd like to shift topics again and turn to the Aventail software.
MR. BOBROW: And, Chris, if I may ask you to put up Slide 18 from the PowerPoint.
Thank you.
Q. (By Mr. Bobrow) I believe that Mr. McLeroy showed you this -- I believe I took my notes down correctly. I believe it was this slide and asked you some questions about that.
Do you remember that line of questions and answers?
A. Yes, I do.
Q. And Mr. McLeroy was somehow suggesting that you were moving things around and changing up clients on us.
Do you remember that line of questioning?

A. Yes, I do.

Q. Now, if you take a look up on -- well, I won't ask you to strain your neck and look up there. You look at the monitor, but if the ladies of the jury look over here next to the words proxy chaining and above Server 1, it says Server 1 appears as a user to Server 2.

Do you see that?

A. Yes.

Q. Can you please explain to us what that means and how that pertains to whether or not something can be a client at one time and a server at another?

A. Basically, what this says is that Server 1 is acting as a client to Server 2. It's acting as a user.

So, for example, this Aventail -- that didn't work; I wanted an arrow.

What's on the left is acting as a client to the outbound server, but the outbound server then acts as a client to this Server No. 2.

Q. And how can that be the case in computer science and in a client/server model? How is it something can be a client at one time with respect to one computer and a server at another time with respect to another computer? How does that work?

A. Well, client/server is a relationship. In fact, we can all see this in our lives.

Sometimes we're the clients, and sometimes we're the servers. And yet we're still just one person. It's a relationship between someone asking for information and someone providing it.

Q. All right. Thank you.

MR. BOBROW: Pass the witness.

THE COURT: Any recross?

MR. MCLEROY: No, Your Honor.

THE COURT: All right. Thank you. You may step down.

All right. Ladies of the Jury, that completes our week. I want to compliment y'all. You have been an extremely attentive jury. You've been taking notes and paying very close attention to some very tedious testimony. And I want to thank you for your efforts in that regard.

What we're going to do is we're going to recess here in a moment until Monday. I'll ask you to be back here at 9:00 o'clock on Monday morning.

We have about -- we have about three hours, three and a half more hours of the testimony -- no, excuse me. We only have about a little less than three hours of testimony. So we should finish the testimony by 11:30, 12:00 o'clock on Monday.

We will then break for lunch, let you

have lunch, then come back after lunch. I will give you your final jury instructions. You will hear closing arguments. Then you can begin your deliberations Monday afternoon.

So the end is in sight. That's good news. I want you to go home and have a relaxing weekend. Remember my instructions. Don't discuss the case among yourselves or with anyone else. Don't make any independent investigation. Just enjoy the weekend and don't think about this case.

Come back with a clear head Monday morning, and we'll get this wrapped up on Monday for you.

So with the Court's thanks, you're excused for the weekend.

COURT SECURITY OFFICER: All rise for the jury.

(Jury out.)

THE COURT: Please be seated.

Well, I am advised the jury would like to have a nice floral arrangement on the table. I'd like to know who would like to take care of that?

All right. We'll allow both of you to get together and split the cost of the nice floral arrangement, but not anything too gaudy. Just something nice for the spring, I think would be nice. They seem to be settling in and enjoying themselves.

All right. With regard to witnesses, what will we have on Monday?

MR. POWERS: On Monday, Your Honor, there will be some depositions and the final live witness will be Keith Ugone, our damages witness.

And subject to Your Honor -- I think it would be helpful for the parties to hear Your Honor's statement of how much time we have left, because I think we will probably need to be cutting down some of the deposition designations, and we will be doing that over the weekend and then that will close off Defendant's case.

THE COURT: All right. The Plaintiff has used 13 of their 14 hours, and the Defendant has used 12 hours and 10 minutes of their 14 hours. So you have an hour and 50 minutes, and you have an hour.

MR. CAWLEY: Yes, Your Honor. We have one rebuttal witness. That will be Dr. Jones.

THE COURT: Okay. Very well. Anything further?

MR. POWERS: No, Your Honor.

THE COURT: All right. Y'all have a good weekend. We will see you on Monday.

COURT SECURITY OFFICER: All rise.

(Court adjourned.)

* * * * *

CERTIFICATION

I HEREBY CERTIFY that the foregoing is a true and correct transcript from the stenographic notes of the proceedings in the above-entitled matter to the best of my ability.

/s/________________________ ____________________
SUSAN SIMMONS, CSR Date
Official Court Reporter
State of Texas No.: 267
Expiration Date: 12/31/10

/s/____________________ __________________
JUDITH WERLINGER, CSR Date
Deputy Official Court Reporter
State of Texas No.: 731
Expiration Date: 12/31/10

EXHIBIT F11

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VIRNETX	*	Civil Docket No.
	*	6:07-CV-80.
VS.	*	Tyler, Texas
	*	
	*	March 15, 2010.
MICROSOFT CORPORATION	*	9:00 A.M

TRANSCRIPT OF JURY TRIAL
BEFORE THE HONORABLE JUDGE LEONARD DAVIS
UNITED STATES DISTRICT JUDGE

APPEARANCES:

FOR THE PLAINTIFFS:
MR. DOUGLAS CAWLEY
MR. BRADLEY CALDWELL
MR. JASON D. CASSADY
MR. LUKE MCLEROY
McKool-Smith
300 Crescent Court
Suite 1500
Dallas, TX 75201

MR. ROBERT M. PARKER
Parker, Bunt & Ainsworth
100 East Ferguson
Suite 1114
Tyler, TX 75702.

APPEARANCES CONTINUED ON NEXT PAGE:

COURT REPORTERS:
MS. SUSAN SIMMONS, CSR
Ms. Judith Werlinger, CSR
Official Court Reporters
100 East Houston, Suite 125
Marshall, TX 75670
903/935-3868.

(Proceedings recorded by mechanical stenography, transcript produced on CAT system.)

APPEARANCES CONTINUED:

FOR THE DEFENDANT: MR. MATTHEW POWERS
MR. JARED BOBROW
MR. PAUL EHRLICH
MR. THOMAS KING
MR. ROBERT GERRITY
Weil Gotshal & Manges
201 Redwood Shores Parkway
5th Floor
Redwood City, CA 94065

MS. ELIZABETH WEISWASSER
MR. TIM DeMASI
Weil Gotshal & Manges
767 Fifth Avenue
New York, NY 10153

MR. DANIEL BOOTH
Weil Gotshal & Manges
700 Louisiana
Suite 1600
Houston, TX 77002

MR. RICHARD SAYLES
MR. MARK STRACHAN
Sayles Werbner
1201 Elm Street
4400 Renaissance Tower
Dallas, TX 75270

MR. ERIC FINDLAY
Findlay Craft
6760 Old Jacksonville Highway
Suite 101
Tyler, TX 75703

* * * * * *

P R O C E E D I N G S

08:04 (Jury out.)

08:04 COURT SECURITY OFFICER: All rise.

08:04 THE COURT: Please be seated.

08:04 All right. Do the parties have anything before we bring the jury in?

MR. POWERS: A couple of matters, Your Honor.

One is an issue that came up at the pretrial conference, and it was VirnetX's motion in limine regarding our evidence that they had earlier accused of infringement, PPTP, which is now being asserted to be prior art.

And Your Honor granted that motion in limine. At Page 7, you said, I'll look at it closer between now and then. Bring it back up with me prior to trial. I think you're zeroing in on something that would probably be an admission. So if you want to use it to impeach their expert, to raise it now, and that's what we're doing now.

So the basic --

THE COURT: So you want to raise -- oh, yeah. Go ahead. Explain it to me a little further.

MR. POWERS: So the basic issue is this: As Your Honor knows, we're relying on PPTP to be a piece of prior art in the case. It's a Microsoft product that was done in 1996.

We believe that the fact that VirnetX's lawyers originally accused it of infringement and withdrew it only when they learned of the date is evidence that should be allowed to be used in cross-examination of their validity expert on the question of whether PPTP does, in fact, come within the scope of the claims.

THE COURT: Response?

MR. McLEROY: Yes, Your Honor.

The short answer is, we never accused it of infringement. PPTP is not mentioned in our infringement contentions. I believe what Counsel is referring to is a letter that VirnetX's lawyers -- former lawyers sent to Microsoft clarifying the definition of accused features in an interrogatory we propounded to Microsoft.

And as you can see from the context of the letter, as well as the interrogatories themselves, it's a broad definition of accused features that VirnetX used at the very beginning of the case, in November of 2007, to identify every possible infringing feature to do our analysis to see which infringed and which did not.

THE COURT: Okay. Is there a document or something that you would rely on, Mr. Powers?

MR. POWERS: There is, Your Honor. It's Exhibit 3252. I can hand up my copy, if you'd like.

THE COURT: All right. Bring up a copy of that.

And specifically --

MR. POWERS: The specific portion I believe is highlighted in that copy, Your Honor. And it is exactly as Counsel has characterized it. It's their lawyers saying, yes, the accused functionality includes PPTP and L2TP.

THE COURT: And let me see the interrogatory.

MR. McLEROY: May I approach?

THE COURT: Okay. When do you need to get into this with him?

MR. POWERS: It would be with their invalidity expert, who will be on this morning.

THE COURT: Next or --

MR. POWERS: No. It will be in their rebuttal case.

THE COURT: Right.

MR. POWERS: So we have -- it will be an hour and a half at least.

THE COURT: All right. Let me study on it a little bit.

What else?

MR. POWERS: Understood.

Your Honor, there were two offers of proof filed late last night on issues that have been

08:08 previously raised and subject of motions in limine, and we wanted to make those offers of proof and obtain indictment rulings from the Court on them.

08:08 The two issues are, I know, familiar to the Court from the motions in limine.

08:08 One is the question of the reexaminations. And that, of course, is relevant also to the witness coming up. It's relevant to various issues in the case and -- including, particularly, willfulness.

08:08 And so we wanted to obtain a definitive ruling from the Court on that issue.

08:08 THE COURT: It's overruled.

08:08 MR. POWERS: Understood.

08:08 THE COURT: Okay.

08:08 MR. POWERS: And the second one on which we wanted a definitive ruling is the question of Microsoft patents which are covering the accused functionality. On that one, Your Honor had earlier ruled as well. There is one change that has happened during the trial that does affect that issue.

08:08 The change is that their damages expert testified on direct examination that one of the reasons 08:09 he believed some of the licenses he was relying upon were particularly relevant was that they included PNRP patents owned by Microsoft.

So this is now a situation that is different from how it was presented to Your Honor in the motions in limine, because now VirnetX has made -- has affirmatively opened the door to the relevance and relied upon the relevance of Microsoft's patents on the accused functionality.

And, therefore, we think that that opening of the door should allow Microsoft to introduce those patents into evidence.

THE COURT: All right. Response?

MR. CASSADY: Your Honor, I don't think it's actually a fair representation to say that we've done anything outside of what we've always intended for these licenses.

When Mr. Sayles and I argued the admissibility of the MCPP and WSPP licenses, I specifically referred to the PNRP-related technologies that has to go into those licenses. That was Wednesday. Here we are Monday morning. That never got brought up for five days that somehow that opened the door to any issue related to these patents.

Furthermore, Dr. Ugone --

THE COURT: So what are you raising, untimeliness in their --

MR. CASSADY: Well, that's one, Your

Honor, or this is just a hail Mary at the end, that they never thought it was relevant, and they're bringing it in now. That's one.

Number two, Your Honor, Dr. Ugone never talked about these patents in his report. He doesn't specifically refer to these patent numbers. He doesn't specifically refer to the Microsoft technology patents.

Three, Dr. Johnson, who he has to rely on for the technical knowledge of these patents, didn't refer to these patents either with regards to the technology in this case.

THE COURT: But Mr. Reed did.

MR. CASSADY: Mr. Reed said that these patents are related to technologies that Microsoft licenses out.

Now what the Defendant's trying to do is come in and say that these patents are for Microsoft Windows products. So if the Windows product is accused -- or is covered by one of our patents, then it can't possibly infringe this patent.

They're trying to bring in or backdoor in an inadmissible argument based on their own patents.

MR. POWERS: May I respond briefly, Your Honor?

THE COURT: Yes.

MR. POWERS: Mr. Reed went beyond merely saying these are patents that Microsoft licenses out. Mr. Reed attempted to increase the relevance of those licenses in the eyes of the jury by saying that these patents related to the accused functionality, and it was that link that clearly opened the door.

THE COURT: Okay. And for what purpose do you want to introduce these patents?

MR. POWERS: As evidence of Microsoft's patents on its own functionality.

If he's relying on them and introducing them and affirmatively relying on them, the patents themselves should be in evidence before the jury.

THE COURT: But are you -- are you wanting to use them to rebut his testimony regarding the damages issue?

MR. POWERS: In part, yes, but in part, they should be admissible now that he's opened the door. He's opened the door to the relevance of those patents.

THE COURT: But --

MR. POWERS: And one purpose would be to rebut his testimony. One purpose would be that Microsoft --

THE COURT: And what would you rebut about his testimony?

MR. POWERS: The relevance in relationship between those patents and the accused functionality, and to the extent they actually do cover the accused functionality, that's relevant to the jury as well.

MR. CASSADY: Your Honor, the only question that these go to is comparability of the licenses. Mr. Reed testified about the comparability of the MCPP and WSPP license programs.

And he said, one reason they're comparable is they include PNRP-related patents and other technologies. He specifically said that this is what Windows -- or this is what Microsoft uses to license that technology out.

He did not say they're related to Windows. He did not say they're related to server. He did not go into that detail.

Dr. Ugone can easily get on the stand and say that these licenses are not comparable without those patents in his hand, as evidenced by the fact that he never referred to those patents --

THE COURT: I'm not going to allow the patents to be introduced. I will allow Dr. Ugone to testify as to the damages aspect with regard to the patents.

MR. CASSADY: And, so, Your Honor, just so we're clear, you mean he can get up and say that these cover the Windows products, and they cover the products in this case, those patents?

THE COURT: No. No.

MR. CASSADY: Okay. Thank you, Your Honor.

THE COURT: Okay.

MR. POWERS: One housekeeping matter, Your Honor. I think there's an agreement between the parties. In that large list of exhibits that we offered on the first day, Microsoft inadvertently included DX3455, which is a physical hard drive of the source code.

And so the parties have agreed that we'll have a placeholder for that where there will be a picture of the hard drive, and Microsoft will retain the physical hard drive in case it's needed for anything.

THE COURT: Yes. And that should be the practice with any physical objects. Substitute a photograph for it.

MR. POWERS: The last thing, Your Honor, on the housekeeping side, I thought Your Honor might want the times for the depositions that are going to be read today, so you'll have that in advance.

THE COURT: Okay.

MR. POWERS: I'll give you the sequence, if you like. There's going to be four depositions played before Mr. Ugone goes on. Those will be Becker, Hopen, Sterne, and then Kindred, and then Dr. Ugone will go on.

And then the final two witnesses will also be by deposition. That will be Victor Larson with an O and then Kindell Larsen with an E. And the times for all of those depositions are 50 minutes for Microsoft, 5-0, and 17 and a half minutes for VirnetX.

THE COURT: Okay. Very good.

All right.

MR. POWERS: I understand that VirnetX's rebuttal case includes two depositions, which as I understand it, are about four and a half minutes.

So the total -- and I think almost none for Microsoft. So the totals for all the depositions will be 50 for Microsoft and about 22 for VirnetX.

THE COURT: Is that correct?

MR. CALDWELL: I think it actually is correct, with the exception of the part that VernetX will not play in its rebuttal case. I think we will play that by ear. So 50 and 17.

THE COURT: Okay. We'll go --

MR. CASSADY: 50 minutes and 17 and a

08:15 half.

08:15 THE COURT: Yeah. We'll do the 50 and the 17 and a half, and you remind me if you put in those two later depositions.

08:15 MR. CALDWELL: Yes, Your Honor.

08:15 THE COURT: All right. Anything further?

08:15 MR. POWERS: Nothing further, Your Honor.

08:15 THE COURT: All right. Bring the jury in.

08:16 (Jury in.)

08:16 THE COURT: Please be seated.

08:16 Good morning, Ladies of the Jury.

08:16 Did you like your flowers?

08:16 JUROR: Yes. Very good. Thank you.

08:16 THE COURT: Well, that's complement of both parties. I told them of your desire to have a -- after such a pretty week, to be locked up in here with no windows all week, I think those flowers are very appropriate, and both Plaintiff and Defendant split the cost of those, and we hope that you like them.

08:16 JUROR: Thank you.

08:16 THE COURT: All right. Very good then.

08:16 Thank you for your jury service last week again. And today is, hopefully, our final day, if we -- we're going to try to work very hard and move through the evidence.

08:16 We have about a little less than three hours of testimony to hear this morning, so we're going to get started.

08:16 With that, Mr. Powers, you may call your first witness.

08:16 MR. McLEROY: Your Honor, may we handle a couple of exhibits?

08:17 THE COURT: Certainly, uh-huh.

08:17 MR. McLEROY: There are two exhibits. We move to admit Plaintiff's Exhibits 985 and 1034. I do not believe there are any objections.

08:17 MR. POWERS: No objection, Your Honor.

08:17 THE COURT: Be admitted.

08:17 MR. McLEROY: And, Your Honor, may I also bring to the front a copy of our exhibits -- list of exhibits admitted Friday?

08:17 THE COURT: All right. You certainly may. That will be accepted without objection.

08:17 MR. POWERS: And similarly, Your Honor, we have a list of exhibits to be admitted today as to which there's no objection and a cumulative list of exhibits admitted through Friday, including the list to be admitted today.

08:17 THE COURT: Any objection to those to be admitted today?

08:17 MR. McLEROY: No, Your Honor.
08:17 THE COURT: All right. Be admitted, and the other list is accepted without objection.
08:17 All right. Who will be your first witness today?
08:17 MR. POWERS: Our first witness, Your Honor, will be Mr. Becker from SafeNet by video deposition.
08:17 THE COURT: Okay. Thank you.
08:18 I'll tell the ladies of the jury, we have four depositions, I'm advised, of four different witnesses coming up, and the runtime on them is going to be a little over an hour, about an hour and ten minutes.
08:18 So just sit back and enjoy.
08:18 (Video playing.)
08:18 QUESTION: Good morning, Mr. Becker. You are Mr. Bill Becker?
08:18 ANSWER: Yes.
08:18 QUESTION: Okay. Thank you very much.
08:18 Mr. Becker, where are you currently employed?
08:18 ANSWER: I work at SafeNet, Incorporated.
08:18 QUESTION: And what is SafeNet, Incorporated?
08:18 ANSWER: It's an information security

company located on -- headquartered in Belcamp, Maryland.

QUESTION: Okay. How long have you been an employee of SafeNet?

ANSWER: Since July 1996, 13 years.

QUESTION: Do you recall that at some period in time, you met with individuals from a company called SAIC?

ANSWER: Yes.

QUESTION: What -- what do you specifically recall about the technology that you were shown?

ANSWER: It was a -- it was a solution to -- they called it EasyVPN. It was a solution to have their software distribute policy to an IP SEC client and IP SEC gateway, and they were trying to make it easier and more intuitive for the end user.

QUESTION: Was SAIC trying to get you at SafeNet interested in their technology?

ANSWER: In some degree, yeah.

QUESTION: Do you recall -- I'm going to show you, in connection with that evaluation, a document bearing Bates No. SAFE-0006. I'm going to mark it as Exhibit 371.

And I'd like to know if this refreshes

your recollection of your conclusions about the EasyVPN technology.
ANSWER: It's an accurate summary.
QUESTION: Does this document, Mr. Becker, appear to be an accurate summary of SafeNet's evaluation of the EasyVPN technology that would have been created in the ordinary course of its business?
ANSWER: Yes.
QUESTION: And what was your conclusion as to whether the EasyVPN technology would actually accomplish the simplicity that it was trying to accomplish?
ANSWER: The concept of -- for the users, it might be simpler, but there was a lot of complexity in the software in actually implementing it, especially with trying to load stuff into a router.
QUESTION: So in your view, would the technology that SAIC had shown you actually accomplish, ultimately, any real simplicity?
ANSWER: No, not really.
QUESTION: Is it accurate, as this memo says, that it seemed that the -- that the complexity it was trying to eliminate had simply been moved from one place to another?
ANSWER: That's accurate, yes.

QUESTION: What exactly does it mean that the complexity that they were trying to eliminate had simply been moved from one place to another?

ANSWER: Their -- the complexity at the time of VPNs was configuring policy of who could talk to who, what different gateways and clients could talk to each other.

So they were trying to simplify it from the user's perspective in that they could just use .scom extensions, and if something was .scom, it would go secure there.

But the complexity would get moved from the user's interface now into their software, and from their software, it would be complex to get it -- to get the keys derived and load it into like a Cisco router or a VPN client.

So they were moving the complexity kind of from the user interface down further into the -- into the networking stack.

QUESTION: So would you call this solution that SAIC claimed to have, would you call it really just something that was, in reality, complex?

ANSWER: Yeah. The implementation was complex, yes.

QUESTION: And do you know whether

SafeNet, in fact, ultimately adopted this EasyVPN technology?

ANSWER: We did not.

QUESTION: Okay. Can you name some VPN companies that have failed?

ANSWER: There's a company called Open Reach that failed. I remember the -- there were -- I don't remember the names of them all. There are a number of them that have disappeared over the years.

QUESTION: Can you estimate how many VPN companies have failed in the market?

ANSWER: A guess is maybe ten.

QUESTION: Is setting up a VPN a hard problem?

ANSWER: It -- it can be.

QUESTION: How can setting up a VPN be a hard problem?

ANSWER: If -- if a user interface or the rules are -- are complex for a -- for a system, it could be hard to -- hard to set up and hard to get operational.

QUESTION: Did you think VirnetX's EasyVPN technology was a bad idea?

ANSWER: No. I didn't -- I didn't think it was a bad idea.

08:24 QUESTION: Just hard to implement?

08:24 ANSWER: It's hard to implement, yes.

08:24 QUESTION: And I think you said that moving the complexity from one place to another -- what did you mean by that?

08:24 ANSWER: I was referring to moving the -- the complexity from -- from the user to the -- to the software that interfaces to load keys into the gateway and into the client.

08:25 QUESTION: So would you agree that EasyVPN technology, once implemented, would make it easier for a user to set up or create a VPN?

08:25 ANSWER: It might compared to certain products, and it might not compared to other products.

08:25 (End of video clip.)

08:25 MR. POWERS: Your Honor, the next witness will be Mr. Hopen from Aventail, and the total time will be 14 minutes.

08:25 THE COURT: All right. You've already given me the times, haven't you?

08:25 MR. POWERS: I've given you the cumulative times, yes.

08:25 THE COURT: All right.

08:25 (Video playing.)

08:25 QUESTION: Can you please introduce

08:25 yourself?

08:25 ANSWER: I'm Chris Hopen. I was a cofounder of Aventail Corporation back in 1996.

08:25 QUESTION: Okay. What were your job titles while at Aventail?

08:26 ANSWER: I ran engineering, so I was Vice President of engineering and Chief Technology Officer.

08:26 QUESTION: What was Aventail Connect Version 3.1?

08:26 ANSWER: Aventail connect 3.1 was a piece of software that would run on an end user's PC that would provide additional secure communications services to applications running on that PC. It would -- it was a client in a pair of a client/server solutions that we sold.

08:26 So it was one component of what we referred to as Aventail ExtraNet Center. And so Aventail Connect was the component that was the client-side software that would be distributed and run on individual users' systems.

08:26 QUESTION: What was the name of the other component of the -- of the Aventail ExtraNet Center?

08:26 ANSWER: Yeah. So, typically, ExtraNet Center was sort of the umbrella name, if you will, for the entire product. The -- I believe at that point in time -- we had a number of different marketing names over the years, and I believe at that time, we would just call that the VPN server component, which was a SOCKS 5-based proxy server.

QUESTION: Can you tell me approximately when the development of Aventail Connect Version 3.1 started?

ANSWER: Well, Aventail Connect 3.0 or 3.X, the 3.X series began -- if you want to go all the way back, the purpose -- one of the main purposes for 3.X was what was called a layered service provider architecture from Microsoft and part of the WinSock 2.0 standard.

That development started, I would say, in late '97, probably -- probably that kind of timeframe, because at that time, Intel and the WinSock community of vendors were working together on a standard.

And so if you -- if you trace it back, you know, that was probably when we began the discussions and design discussions around what would become 3.X or 3.1.

QUESTION: I'd like to mark our first exhibit. I guess we'll mark it Hopen Exhibit 1. It's labeled AVEN 1 through AVEN 124.

And I'd like to ask you, Mr. Hopen, to

08:28 take a look at Hopen Exhibit 1 and let me know if you recognize what that document is.
08:29 ANSWER: Yes. This is -- this is the Administrator's Guide that we shipped with the Aventail Connect and Aventail ExtraNet Center product.
08:29 QUESTION: How was the -- well, was the Aventail Connect Administrator's Guide distributed to anyone?
08:29 ANSWER: It was part of the product distribution that we would distribute to any prospect or -- or end customer.
08:29 QUESTION: Was the proxy chaining deployment ever actually done for a real corporation?
08:30 ANSWER: Yes.
08:30 QUESTION: And what -- what -- what customers did the proxy chaining deployment?
08:30 ANSWER: The two -- one -- you want me to name them or --
08:30 QUESTION: Please.
08:30 ANSWER: Okay. So one of the customers that -- that liked proxy chaining exclusively was a company called DuPont. They had -- as most people know, if you know DuPont, they have many, many subsidiaries in really sort of this -- it's a conglomerate of other companies and brands.

So they had an incredibly complex internal network, and so proxy chaining was one of the only solutions that they could find to solve some of their unique secure-access challenges.

QUESTION: Were there other clients of yours that deployed the proxy chaining?

ANSWER: There were. I mean, certainly, a lot of times, I would only know about it if they had specific questions or issues or challenges around it. A lot of times there -- you know, there was more involvement sort of at the field engineering team level.

I believe Kodak may have been another one that used it extensively. Exxon Mo -- or what were they called at the time? I guess it was just Exxon -- was another company that used it, so...

QUESTION: Okay. Did Aventail ever give betas of Aventail Connect 3.1 to the press for evaluation?

ANSWER: Yes. Yes.

QUESTION: Can you take a look, please, at Hopen Exhibit 2, and let me know what it is?

ANSWER: This looks like a Network Computing article that was written to outline features -- new features and benefits of the Aventail ExtraNet Center solution.

08:32 QUESTION: Can you go down to the fourth paragraph? Do you see the one that starts Network Computing?

08:32 ANSWER: Yes.

08:32 QUESTION: So going through that sentence, it says: Network computing conducted an exclusive test of AEC 3.1 --

08:32 ANSWER: Yes.

08:32 QUESTION: -- and Connect 3.1 betas --

08:32 ANSWER: Yes.

08:32 QUESTION: -- in our real-world labs (R) at Syracuse University.

08:32 ANSWER: Yes.

08:32 QUESTION: Do you see that?

08:32 ANSWER: Yes.

08:32 QUESTION: Was there ever a point in time that Aventail Connect 3.1 was demonstrated at either trade shows or conferences?

08:32 ANSWER: Yes. Yeah, that was commonplace.

08:32 QUESTION: Let me mark another document as Hopen Exhibit 3.

08:32 Mr. Hopen, if you will, please, take a look at Hopen Exhibit 3 and let me know if you recognize what it is.

08:33 ANSWER: This looks like a press release, basically, that we would put out there saying ahead of time, prior to -- looks like this show was the Networld+Interop show. We would put that out prior so that people would see it, and if they were going to the show, that they would know that we were going to be there and stop by and see whatever the latest and greatest was.

QUESTION: Did you go to these Interop shows?

ANSWER: Yes. Yes.

QUESTION: Do you see underneath there it says: Live demonstrations at Aventail ExtraNet Center will be featured at NetWorld+Interop at the Las Vegas Convention Center from May 11 through 13th at the Aventail Booth No. 953 and at the Extranet hot spot Booth No. 8469?

ANSWER: Yes.

QUESTION: Do you -- do you recall whether, in fact, there was a live demonstration of Aventail ExtraNet Center?

ANSWER: Yeah. I believe I was at this actual event. We had this running both -- there was an Aventail booth, which is, you know, a traditional kind of corporate booth that you would see at any trade show.

We would have workstations out front with

08:34 salespeople standing by those workstations. Typically, they would show the Connect client itself in operation, and then they would also show like the Aventail ExtraNet Center Management console and -- and, you know, the user interface and those kinds of things and talk with customers about how they would use it, how they would deploy it, pricing, I mean, you know, any question under the sun.

08:34 The hot spot booth was more of a multi-vendor area where people who had different VPN, Extranet kind of solutions could come and customers could see them side by side and kind of compare and contrast them.

08:35 QUESTION: And if you look at the second sentence there, you see where it says: Aventail ExtraNet Center 3.1 will be available in June, price starting the $7,995?

08:35 ANSWER: Yes.

08:35 QUESTION: And to the best of your knowledge, that's when Aventail started to offer to sell Aventail ExtraNet Center 3.1?

08:35 ANSWER: Yes.

08:35 QUESTION: Okay. Was Aventail Connect Version 3.1 a successful product?

08:35 ANSWER: Yes. Yeah, it was well received.

08:35 QUESTION: Can you give me examples of some of the customers that purchased Aventail Connect Version 3.1?

08:35 ANSWER: The Principal Financial Group, Mass Mutual, Morgan Stanley, Bear Stearns, DuPont, Kodak. I could -- if you give me enough time, I can go on and on and on.

08:35 QUESTION: That's --

08:35 ANSWER: So I don't know how many you want, but...

08:36 QUESTION: Mr. Hopen, are you being compensated today for your time?

08:36 ANSWER: Yes.

08:36 QUESTION: And you're being compensated by Microsoft for your time?

08:36 ANSWER: Yes.

08:36 QUESTION: Are you being compensated at your normal consulting rate?

08:36 ANSWER: Yes.

08:36 QUESTION: With all that in mind, is it your opinion that Aventail was a success as a company?

08:36 ANSWER: So I wore a number of different hats at Aventail, right? I was a founder. I was an employee, right? I was on the board, right? And so it depends on which hat you want me to put on to answer that question.

QUESTION: Let's talk about it from a commercial shareholder perspective. In that sense, do you see Aventail as a commercial success?

ANSWER: I would say probably not. You know, given the same statement, you know, that Aventail -- or that Evan had detailed down here, you know, it was the best transaction for the investors. Would I call that a success? No.

QUESTION: Did Aventail apply for any patents on its 3.1 product?

ANSWER: I don't believe so.

QUESTION: Version 3.1 of Aventail Connect could set up secure encrypted connections, right?

ANSWER: Yes.

QUESTION: It could also be used to set up non-encrypted --

ANSWER: Correct.

QUESTION: -- connections?

And when the host name request is received by the Aventail Connect software, it makes a determination of whether or not redirection rules apply?

ANSWER: Correct.

QUESTION: But just because a redirection rule applies does not necessarily mean that it's going

to be ultimately an encrypted connection, right?
ANSWER: Correct.
QUESTION: All right. The redirection rule is applied, and at that point, Aventail Connect software returns an IP address to the application?
ANSWER: Yes.
QUESTION: At that point, it hasn't tried to contact the Aventail server?
ANSWER: For -- for that particular application, correct.
QUESTION: And then the application, after it receives the IP address, it may or may not send a connection request back to the Aventail Connect software, right?
ANSWER: Yes.
QUESTION: And --
ANSWER: It's part of the standard sockets API.
QUESTION: If it never sends a connection request, no connection, secure or otherwise, will be established, right?
ANSWER: Correct.
QUESTION: Would you agree that it's possible there are people out in the industry who don't think SOCKS is a VPN protocol?

ANSWER: Yeah.
QUESTION: And in 2000, do you think it's pretty likely that there are people out there who thought that SOCKS was not a VPN protocol?
ANSWER: Sure, yes.
QUESTION: In the Aventail 3.1 product, did you ever consider using -- let me back up.
Have you ever heard of IP SEC?
ANSWER: Sure.
QUESTION: You've heard of L2TP?
ANSWER: Yes.
QUESTION: Those are VPN protocols, right?
ANSWER: Yes.
QUESTION: Did Aventail ever consider using any of those protocols in place of SOCKS?
ANSWER: Not until -- in the early, I would say probably not until 2002 maybe, somewhere in that timeframe. But, yeah, not until later.
QUESTION: Not in conjunction with the 3.1 release?
ANSWER: No.
QUESTION: Domain names that were used in Aventail 3.1 were all standard domain names, right?
ANSWER: Yes.
QUESTION: They could all be resolved by

08:39 standard DNS?

08:39 ANSWER: Yeah. We didn't manipulate domain names, I don't think, in any of the products. We would just passively inspect them.

08:40 (End of video clip.)

08:40 MR. POWERS: The next witness, Your Honor, is Mr. Sterne from Trust Information Systems and relating to the DMLP project.

08:40 THE COURT: Okay.

08:40 (Video playing.)

08:40 QUESTION: Good morning, Mr. Sterne.

08:40 Can you please introduce yourself?

08:40 ANSWER: My name is Dan Sterne. I'm an employee of Sparta, Incorporated.

08:40 QUESTION: Mr. Sterne, can you give me a brief description of your education starting with college?

08:40 ANSWER: Yes. I earned a bachelor's degree in mathematics at the University of Washington in 1972 and a master's degree in computer science at the University of North Carolina at Chapel Hill in 1978.

08:40 QUESTION: I want to shift gears a little bit and focus on what I believe is a specific example of some work that you did for DARPA.

08:40 Have you ever heard of a project called

Dynamic Virtual Private Network or DVPN?
ANSWER: Yes.
QUESTION: Can -- was DVPN -- was the DVPN project a DARPA project?
ANSWER: It was funded by DARPA, yes.
QUESTION: Were you involved in the Dynamic VPN project?
ANSWER: Yes, I was.
QUESTION: Okay. And what was your role?
ANSWER: I was the team leader for the effort. I conceived, working with a couple of other people, of the idea and oversaw its prototype and development through its lifetime.
QUESTION: What was Dynamic VPN?
ANSWER: DVPN was an attempt to find a more flexible and scalable way of allowing separate networks to be unified in a way that the boundaries between them, even if they were separated geographically and so forth, would become very transparent so they would be -- have the effect of being part of one network.
QUESTION: The --
ANSWER: Can I add to that?
QUESTION: Sure. Of course.
ANSWER: And -- and what we sought to do

was make it much easier, much more automated, find a more automated -- sorry -- more automated way of doing that in a way that was very flexible and dynamic.

So the goals were basically to allow this kind of marrying of separate networks into a unified network to be done rapidly without a lot of advance planning and with minimal human intervention.

QUESTION: When did you start the DVPN project?

ANSWER: I would probably double-check my notes, but I think it was early in 1997.

QUESTION: Okay. I'd like to mark as Sterne Exhibit 2 a document labeled Sparta 1808 through 1811.

Mr. Sterne, I'd like you to take a look at Sterne Exhibit 2 and let me know if you've ever seen it before.

ANSWER: I have.

QUESTION: Can you tell me what it is, please?

ANSWER: This is an e-mail exchange between Domenic Turchi and myself with other people being cc'd. This is an attempt to describe the highlight of the design of VPN and to talk about some of the technical details of how it would work.

QUESTION: And when was this document created?

ANSWER: October 28th, 1997.

QUESTION: And was it created by Mr. Turchi?

ANSWER: It -- it was in the sense that this particular document was created by him; however, this was probably the result of several iterations between myself and Domenic Turchi.

QUESTION: So does the firewall then make the decision as to whether to create a VPN?

ANSWER: Yes, it does.

QUESTION: And what actually creates the VPN? Is it -- I'm sorry. Is it the firewall that actually then creates the VPN after it makes a decision?

ANSWER: Yes.

QUESTION: Did TIS ever demonstrate Dynamic VPN at any IFDs or IFEs?

ANSWER: Yes. It was demonstrated at IFD -- I think it was 1.1. It was the first IFD. It was then -- that particular technology was then kind of put on hold for a while, and then I believe it was shown at one of the later IFEs. I believe it was 3.1, but I would need to double-check my records to be sure.

QUESTION: I want to mark some more

08:45 documents, if I may. Let me mark as Sterne Exhibit 7 a document -- a document labeled Sparta 1844 through 1854.

08:45 Mr. Sterne, if you could please take a look at Sterne Exhibit 7. I don't know if you've seen it before.

08:45 ANSWER: I have.

08:45 QUESTION: Can you tell me what Sterne Exhibit 7 is, please?

08:45 ANSWER: Yes. It is a description of the configuration of all the computer networking gear used in the IFD, IFD 1.1 with certain areas highlighted to show the components that were being used for some portion of the demonstrations.

08:46 QUESTION: To the best of your knowledge, does the first page of Sterne Exhibit 7 describe the Dynamic VPN demonstration that the TIS did at IFD 1.1?

08:46 ANSWER: I believe so.

08:46 QUESTION: Who was the individual, to the best of your recollection, who actually demonstrated Dynamic VPN at IFD 1.1?

08:46 ANSWER: It was probably Domenic Turchi. Again, Darrell Kindred would be the only other person, and I don't believe Darrell was involved at this point.

08:47 QUESTION: Now, the Dynamic VPN prototype appears to have evolved over time. Would you agree with that?

ANSWER: Yes.

QUESTION: So when it comes to actually how it was implemented, that's something that is not within the scope of -- of your definitive authority?

ANSWER: Well, I would say, after 10 or 12 years, I'm not sure I remember those details very well. Darrell Kindred, who did the programming, can tell you with greater accuracy. I can give you conceptually how I believe it works, but I may not be a hundred percent correct.

QUESTION: So the implementation details would have changed over time?

ANSWER: They -- implementation details would have changed over time, though not necessarily because the concept or the underlying ideas changed. It's just that the prototype is a partial implementation of the idea.

You kind of develop the things that you think are most interesting to a particular audience, and then it -- as time and money permits, you then backfill and, you know, create the other missing pieces. But that's the nature of prototyping, is you generally pick some things that you implement and some things that you don't, at least initially.

QUESTION: Do you think you're the best person to answer those questions, those implementation questions?

ANSWER: No.

QUESTION: And again, in order to know exactly what was demonstrated in the spring of '98, you'd need to look at the source code?

ANSWER: To know exactly what was demonstrated, yes.

QUESTION: Now --

ANSWER: Let me -- let me clarify that.

That would wouldn't be authoritative either because the demonstration didn't show everything that was in the implementation.

QUESTION: And turn again to this figure, Sparta 1513. It's Dynamic Security Perimeter - Establishing VPN.

ANSWER: Okay.

QUESTION: You see the domain names that are in that box in the bottom left?

ANSWER: Yes.

QUESTION: Are those standard top-level domain names?

ANSWER: I'm not sure I understand the question.

QUESTION: Do you know what a top-level domain name is?

ANSWER: Sure, like .com and .mil.

QUESTION: Right.

ANSWER: Sure. .mil is a top-level domain name.

QUESTION: Is it a standard top-level domain name that would be handled by an IETF-compliant domain name service?

ANSWER: I believe so.

QUESTION: And you understand what I mean by an IETF domain name service?

ANSWER: You're talking about conformance to a standard protocol.

QUESTION: Correct. So the domain names that are being referred to on this page of Exhibit 5 all possess standard top-level domain names, correct?

ANSWER: In this example, yes.

QUESTION: Was DVPN, Dynamic Virtual Private Network, as described in your paper, Exhibit 14, was that ever sold as a commercial product?

ANSWER: Not to my knowledge. Not -- not by my organization.

QUESTION: To your knowledge, was it ever sold by anyone?

ANSWER: Not to my knowledge.

QUESTION: Did -- did you ever seek or apply for any patent protection in connection with any of the ideas that were expressed in Exhibit 14 relating to Dynamic Virtual Private Networks?

ANSWER: No.

(End of video clip.)

MR. POWERS: The next witness, Your Honor, is Mr. Kindred, who worked with Mr. Sterne on the DVPN project.

(Video playing.)

QUESTION: Good afternoon, Mr. Kindred.

Can you please introduce yourself?

ANSWER: I am Darrell Kindred. I'm an employee currently here at Sparta, and I was in the -- previous to my employment at Sparta, I was employed at McAfee, which was at times known as Network Associates, as a senior research scientist there.

QUESTION: What is your current job title at Sparta?

ANSWER: Senior research scientist.

QUESTION: Okay. When you joined Network Associates, was there a particular project that you were assigned to?

ANSWER: The first project that I was

assigned to after joining was the Dynamic VPN project.

QUESTION: Who -- when you joined, who was the -- the leader of the DVPN team?

ANSWER: Dan Sterne was the leader of the -- I mean, DVPN was one project under a general contract that Dan was -- was the project manager for, so he was directing the work.

QUESTION: And what was your role on the Dynamic VPN project?

ANSWER: I was the -- you know, at that point, I guess I was basically the lead developer, I would say, or the only -- the only developer, really, on the project at that time.

So Dan asked me to, you know, look into this code and -- and, you know, get it working on a -- in a -- and -- you know, and prepare it for being demonstrated at other facilities.

QUESTION: And let me mark as Kindred Exhibit 1 a disk -- CD of -- a CD labeled Sparta 2236-1.

Is that code dated in Kindred Exhibit 1?

ANSWER: So there are a few ways that I can -- that I can say it's dated. The files in this directory have modification times that would be updated anytime that that file is modified.

And in most instances, these modification times that I'm looking at in the DVPN D folder, for example, are February 1998, March 1998. There are a couple back in November of 1997.

You know, I could look at other files in here, but...

QUESTION: Now, can you describe for me the process of setting up a VPN, for example, from the Red Cross LAN to the FEMA LAN starting with a host on the Red Cross LAN who wants to communicate with a host who's located on the FEMA LAN?

ANSWER: Okay. And again, I'll be referring to the original implementation from '98 or thereabouts.

QUESTION: Please.

ANSWER: So a host in the Red Cross LAN wants to communicate with a host in the FEMA LAN. So I'll use it as an example that there might be a web server in the FEMA LAN that someone with a web browser in the Red Cross LAN may want to access.

They would type into their browser a URL that includes a host name for this host in the FEMA LAN. They would enter that into their browser. The browser or the operating system would then initiate a DNS request to find the IP address that corresponds to that host name.

That DNS request would go to the local Red Cross firewall first where the DVPN agent would intercept that DNS request. The DVPN agent would then forward the request to the domain name server.

I believe that was -- there was typically a standard domain name server on the firewall itself, so the DVPN agent would -- would basically proxy that DNS request and relay it to the local server, which would then send the request wherever it needed to be to -- to resolve the name so that that local DVP -- that local DNS server on the firewall might already have the information cached, it might already know what IP address corresponded to that name, or it might have to go to a server, say, at the FEMA LAN or elsewhere to resolve that name.

When the response to that request comes back, it, again, comes back from the local DNS server on the firewall to the DVPN agent. The DVPN agent inspects the response and looks -- because the response is going to have a -- the IP address of that remote server in it.

Okay. So that would be an IP address within the FEMA LAN. The DVPN agent will look at that IP address and -- and attempt to determine whether that address is inside a community member, coalition member enclave in this case.

In order to do that, the information on who the enclave members are is stored in DNS as well, but this is a different DNS zone that is maintained or for which the master for that DNS zone is the Community Manager.

It's going to retrieve information from -- from -- either directly from the Community Manager or may already have it cached as to who are the members of the enclave. If any of those enclave members -- you know, each of -- each of those records for the enclave members will include a specification of what's the subnet, what's the IP address range that sits behind the firewall, so whatever is the range of firewall addresses within the FEMA LAN, for instance.

So the DVPN agent will notice that the response to the DNS request is an IP address from that LAN. It will notice that it has not already configured a VPN tunnel to that FEMA firewall. It will then rewrite configuration of the configuration file that is -- that is read by the VPN software that's part of the firewall.

It will write the new information in there that the firewall needs in order to establish the VPN tunnel with the FEMA firewall, and the -- and it will then signal the local firewall, the local fire -- the local VPN process on the -- on the Red Cross firewall to reread its configuration, and upon rereading its configuration, it will initiate negotiation of a VPN tunnel with the FEMA firewall.

So that is the VPN agent in the -- I'm sorry -- the -- yeah -- the VPN component in the Red Cross firewall will initiate negotiation of a tunnel with the corresponding software on the FEMA.

Meanwhile, the VPN agent, which has received this -- this DNS response back, will relay that response back to the host that requested it inside the fire -- inside the Red Cross LAN.

The Red Cross LAN host will now have the IP address that it needs to send the actual request to the web server to ask for whatever web page it wanted.

That request will go out to the firewall and through the tunnel that has been established to the FEMA firewall where it will be -- come out of the tunnel at that end and be relayed on to the server in the FEMA network.

And at that point, the client in the Red Cross LAN and the server in the FEMA LAN are able to communicate securely through this VPN tunnel that's been established between their firewalls.

QUESTION: So the name itself for the --

the domain name that's associated with what you had referred to as the FEMA server, that domain name didn't trigger the VPN being initiated; it was a response to that domain name request; is that right?

ANSWER: The request -- the request and the response are both intercepted. The response is what contains the information necessary to determine whether, you know -- the DMLP agent uses information out of the response to determine whether -- as part of the information that needs to determine whether a new tunnel needs to be set up.

(End of video clip.)

MR. SAYLES: May it please the Court.

At this time, Microsoft calls Dr. Keith Ugone --

THE COURT: Okay.

MR. SAYLES: -- its damages expert, and he has not been sworn.

THE COURT: Dr. Ugone?

MR. SAYLES: May I approach and hand up the exhibits?

THE COURT: Yes, you may.

COURTROOM DEPUTY: Please raise your hand.

(Witness sworn.)

MR. SAYLES: May it please the Court.

THE COURT: Proceed.

KEITH UGONE, Ph.D., DEFENDANT'S WITNESS, SWORN

DIRECT EXAMINATION

BY MR. SAYLES:

Q. Dr. Ugone, everyone in the courtroom knows that we're under time constraints, so let's go to work right away, without diminishing the importance of your work, all right?

A. Okay.

Q. And let's work rapidly.

Tell us your name, please.

A. My name is Keith Raymond Ugone. Last name is spelled U-G-O-N-E.

Q. Where do you live?

A. I actually live in Grand Saline, Texas. If you've ever been to Trade Days on I-20 there in Canton, I live the next exit over.

Q. How long have you lived in Texas?

A. Lived in Texas since 1994, sir, about 16 years.

Q. Have children?

A. I've got two sons. Son No. 1, Kyle, is a captain in the United States Marine Corps, and Son No. 2, Casey, lives with me and goes to Tyler Junior College.

Q. What do you do for a living, sir?

09:03 A. I'm actually an economist. Sometimes I'm referred to as a forensic economist, and I'm also a damage quantifier.

09:03 Q. Would you tell the ladies of the jury what a forensic economist or a damage quantifier is.

09:03 A. The easiest way to think about it is, is that companies like VirnetX and Microsoft sometimes get into commercial disputes, and one of them is claiming wrongful conduct and claiming they've been monetarily damaged.

09:03 So someone has to evaluate the amount of the alleged monetary damage, and that's what I do as a damage quantifier.

09:03 Q. And what was your assignment in this case?

09:03 A. I really had two assignments. One was to independently evaluate VirnetX's claim damages should the '135 patent and the '180 patent be found to have been infringed by Microsoft and also that those patents are found to be valid.

09:04 So if those conditions hold, I have an opinion as to the monetary damages suffered by VirnetX, but I was also asked to evaluate the opinions that Mr. Reed presented in court as to what he felt VirnetX's damages were.

09:04 Q. And before we get into the work you did on this matter, tell us about your educational background.

A. I have the slide here. I've got my undergraduate degree in economics from the University of Notre Dame in 1977, and I have a master's degree from the University of Southern California, which I received in 1979. And I got my Ph.D. in economics from Arizona State University in 1983. So I went to college for 10 straight years.

Q. Would you tell us a bit about your work experience after you got your Ph.D.?

A. Well, after I got my Ph.D. in 1983, I worked at one of the California State University systems schools, California State Northridge, for a couple of years.

But then in 1985, I joined PriceWaterhouse, which I'm sure you've just heard of them, the company that counts the Academy Awards ballots. But I worked for them for 18 years, from 1985 all the way up to 2003.

At the very end of 2003, I joined Analysis Group, and I've been there ever since. So about six or seven years.

Q. Have you done this type of work in patent cases before?

A. Yes, I have.

Q. And have you testified in patent cases before?

A. Yes, I've testified in patent cases.

Q. Have you done this type of work for some companies that the jury might have heard of or be familiar with by name?

A. Yes. I've done this work in the past for Microsoft. I have done this work for Samsung. I have done this work for AOL, for Electronic Data Systems. I have done this work for TiVo. So a large number of companies that people have heard of.

Q. Let's get to your assignment. What did you do to prepare yourself to give the opinions that you hold in this case?

A. Well, we can see a slide here that shows a listing of the documentation I reviewed. Actually, there are many, many more documents than this. This is just an overview.

But you can see I looked at Microsoft documents, VirnetX -- VirnetX documents. I considered the trial testimony; I was reading deposition transcripts; I had interviews with Microsoft employees; I had interviews with Dr. Johnson. You can see everything that I reviewed. This is probably a good summary of that.

Q. Now, you heard Mr. Reed testify about the materials that he reviewed.

Essentially, did you and Mr. Reed have access to the same materials?

A. Yes. We would have had access to the same materials.

Q. Now, as an initial matter, let me ask you this before we get started.

From an economic perspective what happens if the jury finds that Microsoft does not infringe these patents?

A. Well, if Microsoft is found not to infringe the patents in dispute here, then from an economic perspective, there's been no monetary harm to VirnetX, so there would be no damages.

Q. And if the jury finds these patents invalid, from an economic standpoint, what does that mean?

A. And so that would, again, lead to the situation where there's no monetary damages in that situation.

Q. All right. Now let's go to your opinions. Before we get into the details, give the jury an overview of what your opinions are?

A. Sure. I have a couple of opinions. First one is is that Mr. Reed, in his presentation, has significantly overstated VirnetX's claim damages.

The opinions I hold is that the parties, if they had negotiated a license to the patents in dispute here, would have negotiated a lump-sum payment structure and the payment would have ranged between $9 million and $15 million for a license to the two patents in dispute here.

Q. Mr. Reed did a Georgia-Pacific analysis to determine the royalty payment that he testified about in his testimony, and you were here for that?

A. Yes.

Q. Essentially, did Mr. Reed describe the framework of a Georgia-Pacific analysis properly?

A. Yes, he did. There's 15 Georgia-Pacific factors, and I'm not going to dispute his presentation. I think those are generally accepted factors.

Q. All right. So we won't go into details about explaining those factors except as they relate in other ways to your opinions. But did you do a Georgia-Pacific analysis?

A. Yes.

Q. Now, Mr. Reed conducted what is known as a hypothetical negotiation analysis; is that right?

A. Yes.

Q. Did you also perform a hypothetical negotiation analysis?

A. Yes, I did.

Q. In doing that in the legal framework you are to follow, are you required to make any assumptions?

A. I have and I have a slide on that, and you can see a negotiating table here. And it's a hypothetical negotiation because the parties did, in fact, not negotiate a license in the past, but I am required to make certain assumptions, which I have listed on the -- the right side of the chart there.

Some of the assumptions I am required to make are that the patents are valid, enforceable and infringed. And that the parties, both VirnetX and Microsoft, would have a willingness to negotiate, that VirnetX would be willing to give a license to the patents we've been talking about and that Microsoft would be willing to acquire a license.

But what's important is in this hypothetical negotiation is that the parties go into the negotiation as prudent business people. They go in smart. They have knowledge as to the relevant economic factors to help them determine the appropriate royalty payment for the use of the patents, and they have reasonable expectations as to future events.

And then finally, I think as the jury has understood, nobody can kind of leave this room without having reached an agreement, so they must reach an agreement.

09:10 But this is the general framework of the hypothetical negotiation.

09:10 Q. In a hypothetical negotiation, can one side dictate to the other the outcome?

09:10 A. Well, the best way to think about it is we're trying to determine a reasonable royalty payment, and so what that means is one side can't dictate the outcome. There has to be the inner play between the negotiations to determine this reasonable payment.

09:10 Q. Now, in the context of a case like we have here, you are required to do this hypothetical negotiation framework because that's the legal method in which you do it; is that right?

09:10 A. Yes.

09:10 Q. But do the real world facts count?

09:10 A. Yes, the real world facts count. As I said, these are business people going into the negotiations, and so there would have been relevant financial information and economic considerations at the time of the hypothetical negotiation. So even though it's a hypothetical negotiation, you're still using real world information and real world economic considerations.

09:11 Q. And let's talk about the hypothetical negotiation. Remind the ladies of the jury when it would have taken place.

A. Well, it would have been in early 2003 or March 2003. That's the time of the alleged first infringement, so that's the point when Microsoft would have required a license to the patents-in-suit, so that's when the negotiations would have taken place.

Q. Between which parties?

A. And at that time, SAIC owned the patents that have been discussed here, so it'd be between SAIC and Microsoft. So, hopefully, I'm not hitting this too much. I don't know if that's disturbing to people.

Q. Could you tell us what would have been discussed at the negotiation, what topics?

A. Well, what I'm really here to present is the economic questions that would be answered at the hypothetical negotiation, and I've kind of hinted at these.

But there's really two primary ones. The first one is what's the payment structure for a license to the patents-in-suit, and the second one is what's the payment amount. So how much is going to be paid and what are the -- what's the structure of those payments. Those are two important economic questions to be addressed.

Q. And what types of payment structure are there?

A. Well, I've got a slide that shows two of them.

There's actually various combinations, but it's easiest to think about these two. The first is called a lump-sum payment structure, and a lump-sum payment structure, as the slide says, is just sort of an upfront paid-in-full royalty payment.

So the parties negotiate. They determine the amount of the pavement as paid upfront and then you have a license and a freedom to operate using the patents that have been licensed, so it's one-time payment.

The second type is called a running royalty, and the easiest way to think about that is that that's one that's -- could be based on volume. So if the volumes go up, there's higher payments; if the volumes go down, there's lower payments. So there can either be a lump-sum upfront payment or there can be a running royalty payment.

Q. Now in this case --

THE COURT: Excuse me, Dr. Ugone. You may want to lean back a little bit or move that. You can move that microphone out a little bit. It's sort of bent around there. You're popping a little bit.

THE WITNESS: Okay.

Q. (By Mr. Sayles) Now, in this case you know Mr. Reed is contending for a running royalty, right?

A. Yes.
Q. And your opinion is that there would have been an upfront paid-in-full royalty?
A. That's correct.
Q. And are there advantages and disadvantages to either structure?
A. Sure. Yes, there's -- depending on sort of the facts and circumstances and -- and the economic circumstances surrounding the businesses and the license, that dictates which of these makes sense. So yes, there are advantages and disadvantages to both.
Q. All right. Now let's talk about the hypothetical negotiation. And could you tell the jury what economic factors would have been important in a hypothetical negotiation between SAIC on the one hand and Microsoft on the other?
A. Well, I'm going to go through six topics of discussion. I'm going to briefly touch on the thousands of features and functionalities contained in the accused software products; I'm going to talk about the usage of the accused functionalities; I'm going to talk about Microsoft's patent licensing practices; I'm going to talk about SAIC's failure to commercialize the SAIC technology.
And I think we've -- the jury has heard of

this. We're only going to talk about the SAIC licenses with SafeNet and VirnetX, and I'm also going to talk about certain value indicators that existed over time.

Now, some of these things you've already heard of, but what I'm going to try to do is take these and put them in the context of the hypothetical negotiation so you can see how these would be used in the negotiating process to determine a reasonable royalty payment.

Q. All right. Let's start with the first one.

Can you explain the economic significance of the fact that there were thousands of features and functionalities in the products that are accused here?

A. Well, this -- from just listening to trial throughout the past week seems to be undisputed, especially when you talk about Windows XP and Windows Vista, that there's many, many basic, but important features and functionalities in those operating systems.

And I think you've seen some of the witnesses use a computer. Well, the operating system helps the computer recognize the keyboard or the operating system, allows the text and the graphics to be displayed on a monitor. The operating system helps the computer recognize a printer so you can print documents. Those are all important features and some of the thousands of features that are included in the operating systems in XP and Vista that we've been talking about up. And I think as we've also heard that there's many, many hundreds, if not thousands, of APIs as well.

Q. And from an economic standpoint, what is the significance of that?

A. Well, the significance of that is if you look at the complexity of the product, that with XP and Vista, for example, there's these thousands of functionalities, and what the parties are negotiating over are just some limited features or functionalities within this much larger software product in a sense.

Q. The next economic consideration you mentioned that you would discuss is the usage of these accused functionalities. Would you explain that, please?

A. Yes. And this would be important to the negotiators at the -- at the hypothetical negotiation. And I have a slide on this one as well.

But when I'm talking about usage, what I'm really looking at, first of all, is sort of the usage of the accused functionalities relative to the usage of just the XP and Vista operating systems in general. And relatively speaking, obviously, these accused functionalities are used in a much more limited sense than the entire operating systems.

But in this example here, I just tried to give a little bit of an idea of that, that over -- if you look from 2003 to 2008, there were roughly 280 million copies of XP and Vista in the United States. But at the same time people that had client access licenses that allowed LCS and OCS to be used with XP and Vista, so those were licenses that would allow, in a sense, a combination of these software products, were only about 15 million dollars -- 15 million copies. If we roundly look at those numbers, 14.8 million.

The point is that's much less than the 280 million, and that would be important to the negotiators at that negotiating table.

Q. Dr. Ugone, I'm going to point out above your head here the right-hand corner where there's a DX number there.

Are there exhibit references on the graphics that you've prepared to explain your testimony?

A. Yes.

Q. And so this data comes from information that was available to you and Mr. Reed?

A. That's correct.

Q. Now Mr. Reed concluded that had Microsoft would agree to pay royalties relating to the '135 patent for each and every copy of Windows XP and Vista?

A. That's correct. So he's -- he is calculating royalties on the big blue bar, even though it's -- it would be the -- my understanding -- for the alleged infringement, that there would have to be this combination of -- for the '135 patent XP and Vista with LCS and OCS.

Q. Do you agree with Mr. Reed's conclusion?

A. No, I do not.

Q. Why not?

A. Well, if you think about it, if you are a business person at the negotiating table, while you're negotiating a license to the '135 and the '180 patent, you know that there's an awful lot of copies of XP and Vista that are not going to be used in an alleged infringing way, and so that's going to be an important economic consideration at the hypothetical negotiation.

Q. For the '135 patent, if one must use LCS or OCS with XP or Vista in order to use the functionality that's accused, have you done the math to see what that usage is?

A. Well, you would -- if you do a division here, you get about 5.3 percent.

Q. And what is it that Mr. Reed did in this regard?

A. Well, he was applying a royalty rate to all the copies of XP and Vista, the revenues associated with them.

Now, I have to be a little careful. He did some adjustments. If you recall, I think he had 40 -- 44 to 48 billion dollars of sales. He adjusted that down ultimately to 30 billion, but it's still a substantial number of the XP and Vista copies.

Q. So let me see if I understand this correctly. Is it your opinion that Mr. Reed thinks Microsoft would have, at the table, agreed to pay a royalty on over 250 million copies of XP and Vista even though both parties would know those copies wouldn't infringe the '135 patent?

A. Well, he -- yes, he essentially is -- is giving that opinion.

Q. And do you agree with that analysis?

A. No, I do not.

Q. And from the standpoint of the hypothetical negotiation, tell us briefly why not.

A. Well, again, think about what a -- what prudent business people would do. And this is from an economic perspective. And from an economic perspective, you'd be looking at the limited usage of the features that the license would be required to have Microsoft provide to its customers, and those are much more limited than all the copies of XP and Vista.

So a prudent business person would not agree to paying royalties on all the copies of XP and Vista even with some adjustments; and frankly, SAIC on the other side of the negotiating table, if you think about it, would have reasonable expectations as to the royalty base as well. So they would be taking that into account as well.

Q. I want to shift your attention now to the claims of the '180 patent and the feature of PNRP Plus Grouping. Regarding this usage idea, do you have a similar opinion?

A. Yes. And -- and we've heard some of this testimony, that there are no applications using the PeerNet APIs for Windows XP. We've heard testimony that there was only one application, Windows Meeting Space, that used the PeerNet APIs and -- in Windows Vista. And if we get a little bit more technical about it, there was some discussion about a PNRP Plus Grouping functionality in a sense, but that was rarely, if ever, used in conjunction with Windows Meeting Space.

So, again, the point is, like I was saying before, but now we're looking at the PeerNet APIs that, again, there's limited usage and the parties realistically would not expect to have a huge royalty base or payments on a huge royalty base when there's much more limited usage of those functionalities.

Q. And the parties would know that at the negotiating table?

A. Yes.

Q. Now let me shift your attention to the other area, the third area that you said you would address and that's patent licensing practices.

Could you describe what you did in this regard, please?

A. Yes. So I looked at 20 Microsoft what's called inbound patent license agreements. And I have to explain that a little bit. But we're -- we're trying to understand what are the licensing practices of the parties at the hypothetical negotiation. So, in a sense, you know, what are their positions going in and how do they like to run their business with respect to licenses to intellectual property.

And we can show a slide here. Perhaps. There we go.

Q. First of all, before you go into that, tell us what inbound means in this context.

A. Right. So we have Microsoft inbound patent license agreements. And think about it as inbound versus outbound. On the inbound ones, it's Microsoft paying the money out to get a license coming in to use those -- whatever patents are involved in the license agreement.

So the inbound patent license agreements I'm going to talk about is where Microsoft was the one acquiring the patent. In other words, they were -- not acquiring the patent, acquiring a license to use the teachings of the patent. That's what we're talking about.

Q. All right. I interrupted you. I'd like you to, using the slide as an aid, describe for the jury the significance of the inbound licenses.

A. Well, what I'm going to do is just give you an overview. There were 20 inbound patent license agreements that Microsoft had entered into. And if you look at those, virtually all of them were non-exclusive. They were software patent license agreements. Generally, they had 10 or fewer patents associated with them. They took place over the 1997 to 2007 time period.

So what we're trying to do here is look at patent license agreements inbound that Microsoft had entered into, really, kind of from an economic perspective to see in those patent license agreements what did they do. And all 20 of those were lump-sum payments that Microsoft made for the use of the teachings of the patent.

Q. And so what is the economic significance of that at a hypothetical negotiation?

A. Well, Microsoft, from an economic perspective, would go into the negotiations and that would be the type of payment structure that they would want for a license to the '135 patent and the '180 patent.

Q. Now let's shift to the failure to commercialize the technology in the '135 patent.

Would you explain what you mean when you say there was a failure to commercialize the technology?

A. Right. And what we're doing here is looking in some of the economic forces or pressures that would have been present at the hypothetical negotiation. And as we've entitled this chart, there was sort of what we call a market rejection of the technology. And we saw that -- and I think the jury has heard this over the past week -- that In-Q-Tel did not want to do any additional funding into this technology; that various government agencies did not want to pay any money to use the technology; that investors and venture capitalists from a market perspective and from an economic perspective were not willing to invest in the technology; that businesses did not want to use the technology. And we've even heard about SafeNet entering into a license agreement with SAIC, but after evaluating the technology for six months, terminated that license agreement.

So what we have here are a series of indicators of the unwillingness of the market to invest in the technology, and that would have been very important.

Q. And what are the economic implications of these failed attempts by SAIC to commercialize?

A. Well, so what you would have is SAIC going into the hypothetical negotiation, in a sense, on the heels of others out in the marketplace unwilling to invest in the technology to provide funding. So that would have been top of the mind to them, and that would have tempered or lowered some of their expectations of the type of payment that they could get for a license to the -- to the use of the technologies we've been talking about here.

And, in fact, the SafeNet rejection of the license agreements I believe occurred in December of 2002, which would have been only months before the hypothetical negotiation in early 2003.

So, from SAIC's mindset, there's sort of a difficult economic situation where no one is willing to -- to invest. And they're going to know from an economic perspective that riskiness associated with this technology. And not only would that temper what their expectations would be, but it would -- also could lead them to the willingness to accept a lump-sum amount.

Now from the other perspective, you have Microsoft that would know these same things, and that would place downward pressure on the amount that they were willing to pay. Because there's been market indicators no one's willing to invest in the technology.

Q. All right. Let's -- let's talk about the license to the patents-in-suit. You heard Mr. Reed identify two licenses to the patents, specifically the SAIC SafeNet license and the SAIC VirnetX license.

What is your opinion regarding those licenses?

A. Well, we have to be very careful with these licenses. There's the SAIC/SafeNet license that Mr. Reed used as a -- as a key benchmark and he talked about the 20 percent. Well, the first thing we have to realize is that was sort of a beginning point that Mr. Reed made adjustments to.

But the point is with the SafeNet license agreement of 20 percent, the safe -- or I'm sorry -- the SAIC/SafeNet license agreement of 20 percent, the

SAIC/VirnetX agreement 15 percent, I think the important takeaway is while those were stated rates in the agreements, there's been no payments. SAIC has not -- did not receive any payments from SafeNet. And, in fact, what SafeNet did was terminate the agreement and did not make any payments.

And I want to be a little careful on the VirnetX license agreement. There were some $50,000 fixed payments that had to be made each year, so I think they might have paid close to $200,000 up to this point, but they have not made any royalty payments related to products. So that's what I mean when I say there's no payments.

But the key is that these were key benchmarks being used by Mr. Reed. But in the sense of a product where royalties have to be made from sales of the product, that has not occurred.

Q. All right. Next, let's talk about the various value indicators that you said you would discuss.

A. Right.

Q. Can you tell us what you mean by this, please?

A. And what I'm looking at here is that if you look at the documentation and if you look at what was happening, and I'm going to say contemporaneously, what were the businesses looking at, how were they valuing things, you can see this sort of timeline across the bottom. And I will just go through it quickly. That SAIC internally around February of 2001, in that time period, was looking at valuating a company that had the SAIC -- SAIC technology at about $15 million.

In-Q-Tel, in their discussions with SAIC, said no that the value's really this point currently. That's what we're talking about, at that moment in time, the value is $10 million.

The venture capitalists were saying back to SAIC at this moment in time, it's worth $12 million. And there's even a document that shows that SAIC was valuing the technology, not a company including the technology, but the technology itself, at that moment in time at $2.7 million.

Q. Let me stop you right there for a moment.

A. Okay.

Q. Now we have on the graph that the ladies are seeing a DX number under each one of these. Are these the documents that support what you're saying here and where these numbers can be found?

A. Yes.

Q. I notice that there are two green bars on the graph. Could you explain what those mean, please?

A. Yes, sir. Two green lines, now a box is above them. But the first of the two tells us in the timeline when the '135 patent issued and that was December of 2002, and then the second green bar to the right of the first one tells us or shows us diagrammatically where the hypothetical negotiation would have been on this timeline. So that's March of 2003.

Q. All right. Now, before we move on, this $2.7 million amount that was put on the value of the technology just before the hypothetical negotiation, is that an SAIC internal document?

A. Yes, it is.

Q. I see a $15.4 million number on the bar in the chart that has Larsen 4/3 below it. What is that?

A. So that was in April 2003. They were discussing a potential spinoff of the technology in the company. And currently at that point in time they were trying to raise some funding, but they put a value at 15.4 million on -- on the company with the technology at this point.

Q. All right. Now, I want to get a little deeper into this one. But first of all, Mr. Larsen is Mr. Kendall Larsen who is currently the Chief Executive Officer and Chairman of the Board of VirnetX, the Plaintiff in this case?

A. That's correct.

Q. But at the time of this document, what that before the formation of the company VirnetX?

A. Yes.

Q. And so is what we have Mr. Larsen negotiating with SAIC?

A. Yes.

Q. Let's take a look at Exhibit 3193 that is shown there. And first, tell us the date of this.

A. That's April 25th, 2003.

Q. And on the second page there is a reference to Kendall Larsen. Do you see that?

A. Yes. It's highlighted in yellow and there's an attachment there, yes.

Q. It says Larsen's cap table indicates our proposed ownership position post funding.

And then is there an attachment that has Mr. Larsen's table?

A. Yes.

Q. Let's look at that.

But on this table in the document there's a figure of 15,384,614. Tell us what that is, please.

A. Well, at the current time that they were negotiating this spinoff company, that was the value they were placing on the company and the technology at that moment in time.

Q. All right. Now, let's go back to your value indicators. I see there is an $18 million value at the end there. Can you tell us what that is?
A. That's in October 2006 and that was negotiations between SAIC and VirnetX, and the concept there was that VirnetX was trying to get SAIC to provide some additional funding for VirnetX, and so they were discussing then what a perceived current value of the -- what the company was at that moment in time.
Q. So, here again, private discussions between SAIC on the one hand and VirnetX on the other?
A. Yes.
Q. Let's take a look at Exhibit 3165 that's referenced there. And can you tell us first what this is?
A. Yes. Again, here's an e-mail October 9th, 2006, and you can see it was from Mr. Larsen.
Q. Kendall Larsen, CEO and co-founder of VirnetX?
A. Yes.
Q. And at this time, does this document show what the perceived value of the company was?
A. Yes, I think if we --
Q. Let's go to the next page.
A. Right. So --
Q. From the document, tell the jury what we're

09:34 seeing here.
09:34 A. Well, you can see a little bit of a difference of opinion, but it ranged from $12 million to VirnetX's proposal of $18 million. But that was the range they were discussing.
09:34 Q. And is this at a time when they even knew they might have legal claims against Microsoft?
09:34 A. Yeah. There appears to be a reference to that. VirnetX leads legal claims for M-Co, which my understanding is Microsoft.
09:34 Q. Have you seen the depositions that explain that?
09:34 A. Yes.
09:34 Q. And even though they knew they may have legal claims against Microsoft at the time, the numbers being mentioned were between 12 million and 18 million between the two parties?
09:35 A. That's correct.
09:35 Q. You have heard Mr. Reed's damages conclusion earlier this week, and let's go back to your value indicators.
09:35 And I -- I see on the right-hand side the number that Mr. Reed presented to the jury. Do you recall that?
09:35 A. Yes, I do.

Q. Is Mr. Reed's damage conclusion consistent with these facts that we've just discussed?

A. No. What's going on here is, again, we've looked at all the economic indicators and economic considerations that would have been discussed at the hypothetical negotiation. And here we have the value indicators and we see them over time that they're stable in this range of, when you look at a company that is incorporating the technology, of around $15 million.

Now we have to be a little bit careful in our comparisons, but what Mr. Reed is saying is around the time of the hypothetical negotiation in 2003, March 2003, he's saying the outcome of the hypothetical negotiation would be that SAIC and Microsoft would have agreed to a running royalty payment structure that would ultimately lead to $242 million in royalty payments from that point to basically the end of 2009 I think it is.

But that is in stark contrast to what the contemporaneous documents are telling us or the documents at the moment in time from 2001 to even 2006. So that's a stark contrast.

Q. You told us earlier that you did your own Georgia-Pacific analysis, and let's take -- here are the 15 factors on the board that I told -- told the jury earlier we wouldn't go into detail into all of those,

but these are the same factors that Mr. Reed put up?
    A.   That's correct.
    Q.   And did you incorporate all of these factors and more into your testimony today?
    A.   Yes. I did a substantial analysis, and I looked at all of these factors and then I summarized my opinions today.
    Q.   And everything that you've discuss today, would both SAIC and Microsoft have known all of these considerations at the time of the hypothetical negotiation?
    A.   Yes. In fact, remember what I said at the beginning. You have a hypothetical negotiation, you have the willingness to negotiate, and you have the reasonable knowledge and expectation such that the parties can go in smart. They're prudent business people. They're prudent negotiators. They would know all of these things in the hypothetical negotiation.
    Q.   Dr. Ugone, what did you conclude based on your analysis of the Georgia-Pacific factors and everything you've discussed today and everything you studied in preparation for your testimony?
    A.   Well, I have reached the conclusion that Mr. Reed has substantially overstated claim damages, and for the reasons that I've provided today, the parties

would have entered into a license agreement at the hypothetical negotiation but it would have had a lump-sum payment structure, and the amount of the payment would have been between $9 million and $15 million.

Q. One final thing. Now, if the '135 patent is found not to be infringed or is found to be invalid but the '180 patent is found to be infringed and valid, what would happen?

A. Well, I've just -- a couple of things would change. So this is if the '135 is not valid or is not infringed but the '180 is found to be valid and infringed, what changes is the date of the hypothetical negotiation moves to March 2007. The parties change. It's now going to be VirnetX and Microsoft. But many of the underlying economic considerations would still be the same.

So even though the date moves forward a little bit and even though it's now VirnetX and Microsoft instead of SAIC and Microsoft, I have reached the conclusion, because of the underlying economic considerations, that the answer would still be between $9 million and $15 million in a lump-sum payment structure.

MR. SAYLES: Pass the witness.

THE COURT: All right. Thank you. All right, ladies of the jury, I think we'll take our morning break at this time. So we're going to be in recess until 5 minutes until 11:00, and I note that our clock has not been moved forward so we -- we are on daylight savings time, and it will be about a 15-minute break. Be in recess.

COURT SECURITY OFFICER: All rise.

(Jury out.)

THE COURT: Please be seated.

All right. Mr. Powers, the Court has taken a look at your reurging of wanting to cross-examine their rebuttal -- Plaintiff's rebuttal witness with the December 17th, 2007 letter from VirnetX's counsel to Microsoft's counsel regarding the point-to-point tunneling protocol and the layer 2 tunneling protocol, and I'm not going -- I am going to stand by my ruling and exclude the letter for cross-examination purposes for the reason that the paragraph that you're referring to is a response to VirnetX's interrogatories.

And in paragraph 19 of their first set of interrogatories, VirnetX identified the accused features and then lists A through S of the accused features. And apparently in response to a meet and confer with

Microsoft's counsel, VirnetX responded back as follows: Without prejudice in an effort to assist you in responding to these interrogatories, the features found in the accused products are as follows. And it lists some more specific features than the accused features in the interrogatory.

But I don't think that that -- if it had have been in their infringement contentions or in a pleading, I would allow you to cross-examine, but I don't think where attorneys are trying to give guidance on discovery would be such an admission and are contrary to our patent rules desire to have meet and confers. And so that will be my ruling on that.

With regard to the Court's charge, we have a draft ready that Ms. Li will be passing out to you, and after we conclude the evidence, I'll hear any objections to the Court's charge.

Be in recess.

MR. CAWLEY: Your Honor, could I raise a quick matter of procedure --

THE COURT: Yes. Uh-huh.

MR. CAWLEY: -- to maybe save some time?

I understand that the Defendant has two depositions to play and that they then intend to rest. We'll have a motion for JMOL that we'd like to make at that time unless the Court would prefer that we all agree to defer that until, I guess, sometime over the lunch hour or -- in order to avoid breaking up the testimony and we're trying to get finished.

THE COURT: If that's agreeable to the parties, we will do that immediately after the conclusion of all the evidence as well.

MR. BOBROW: Yes, Your Honor that will be fine.

MR. CAWLEY: Thank you, Your Honor.

THE COURT: All right.

COURT SECURITY OFFICER: All rise.

COURT SECURITY OFFICER: All rise.

(Jury in.)

THE COURT: Please be seated.

All right, Counsel. You may proceed.

MR. CASSADY: May it please the Court.

CROSS-EXAMINATION

BY MR. CASSADY:

Q. Dr. Ugone -- good morning, Dr. Ugone. My name is Jason Cassady. I think we have met more than a couple of times before, correct?

A. We have, yes. Good to see you.

Q. And as Mr. Sayles said earlier, we're all under time constraints here, and I'm going to ask you to please answer just the question that I ask and to give Mr. Sayles a chance on redirect to come back and clarify anything that he thinks was unfair. Is that fair?

A. I will agree with that, yes.

Q. Okay. Okay. Now, Dr. Ugone, you filed an expert report in this case, correct?

A. Yes.

Q. And I take it we can rely on your expert report to accurately -- accurately portray your opinions in the case?

A. Yes.

Q. And I think you've already actually mentioned it, but your report included an opinion as to damages just for the '180 patent, correct?

A. Yes.

Q. Okay. And then you also said it included an opinion for the '135 and the '180, correct?

A. Yes.

Q. But it was -- it said 9 to $15 million for both of those opinions, correct?

A. Yes.

Q. Okay. So, no matter how many patents are in this case, the answer -- your answer is 9 to $15 million, correct?

A. Yes.

Q. Okay. Now, Dr. Ugone, this isn't your first case that you've worked for Microsoft, is it?
A. That's correct.
Q. Okay. And in this case you're testifying to a lump-sum agreement, correct?
A. Yes.
Q. Well, with that in mind --
MR. CASSADY: Let's go ahead and pull up slide number 2, please.
Q. (By Mr. Cassady) I would like to ask you this question: How many times, including this case, have you testified to a lump-sum on behalf of Microsoft? Would it be once, twice, or three or more times?
A. Actually, I'll take off the four or more times and then it would be accurate to say three times.
Q. Okay. So at least three times then; that's fair?
A. Let me -- if I could ask a clarification. In fact, here, I will help you with the answer: I can remember being retained four times for Microsoft, three times I testified at trial, and in those three times, I gave a lump-sum opinion.
So, it's not at least three times testified, it's three times.
Q. Okay. Fair enough.

Now, sir, you've also testified in cases for the Plaintiff or the patent owner, correct?
A. Yes.
Q. Okay. The patent owner like VirnetX in this case, correct?
A. You took it a little bit farther, but I'm willing to say yes, I've -- I've been retained by a patent holder to evaluate their damages, yes.
Q. Okay. And so -- so isn't it true, Dr. Ugone, that when you've been hired by people that own the patent, which is -- which is seeking a royalty in those cases, a reasonable royalty in those cases, you have never testified that a lump sum was appropriate?
A. Again, I just need a clarification. At trial I've testified as to running royalty rates. I have given opinions in the report where it's a lump-sum amount on the Plaintiff's side as well.
Q. Well, at trial you've never stood under oath and testified for a Plaintiff, a patent owner, that a lump sum was appropriate, correct?
A. That's correct. The facts and circumstances weren't the same.
Q. Okay. Now, sir --
MR. CASSADY: Could we put up slide -- well, actually, I apologize.

Can we put up slide 22, Mr. Moreno?
Q. (By Mr. Cassady) Dr. Ugone, you put this slide up just a few minutes ago and said that this included all the indicators of the valuations of VirnetX or the SAIC technology, correct?
A. I think you've misquoted me. I said they were value indicators. There's obviously additional ones in my report. I was trying to give a representative sample across time, but if that was what you were meaning to say, then I'll agree with that. If you're trying to say that this was all of them, I would say no.
Q. Right. Well, fair enough.
The point is these are the ones you chose to show the jury, correct?
A. Yes.
Q. Okay. And this is not all of the valuations that were done on the VirnetX and SAIC technology, correct?
A. There are some additional ones, yes.
Q. Okay. Well, let's talk about some of those additional ones.
MR. CASSADY: Can you bring up slide 19, Mr. Moreno?
Q. (By Mr. Cassady) Now, Dr. Ugone, can you see here this is a Cambridge Strategic Management Group?

Now, you read the reports by the Cambridge Strategic Management Group, correct?
A. Yes, I did.
Q. Okay. And do you see this bullet point highlighted, it says: Business case analysis indicates a total net eraser, net present value of $190 million.
Do you see that, sir?
A. It says 190 million. I'm aware of this document, and I think there's a lot more going on than what we're showing the jury, but I don't disagree that that's what it says. But also this was not believed by anyone.
Q. Okay. Well, let me just ask you this: You agree that NetEraser is a reference to the technology in this case, correct?
A. Yes.
Q. Okay.
A. Yes.
Q. So, that might as well say business case analysis indicates a total VirnetX net present value of $190 million, correct?
A. I'm sorry. Could you say that again?
Q. You would agree with me that we can replace the word NetEraser in this quote with VirnetX, the VirnetX technology, and that would be accurate still? It's just

a synonym, correct?
A. Yes. If you wanted to do that, you could do that. But, obviously, there's a lengthier document that has some underlying assumptions that were not accurate and that's why this number was not accurate.
Q. Well, I understand that you feel that way, Dr. Ugone, but you didn't show this $190 million valuation to the jury in your analysis and tell them why it's inaccurate, did you?
A. No, but I'd be willing to do that now if you would like.
Q. Well, maybe Mr. Sayles will ask you that.
MR. CASSADY: The next one, Mr. Moreno, is slide 20, please.
Q. (Mr. Cassady) Here's another one by CSMG. And let's just get some backup information on this, Dr. Ugone. CSMG is not SAIC, correct?
A. That's correct.
Q. It's a third-party company that went out and did this valuation, correct?
A. They were doing valuations, yes.
Q. Okay. So CSMG in this one here, they said the net present value was $264 million, correct?
A. I don't disagree with what it says. There I have my same comments about the invalidity of this

number.

Q. Okay. And then --

MR. CASSADY: So let's just -- let's just go ahead and go back to slide 22, Mr. Moreno. 22. I apologize.

Q. (By Mr. Cassady) Now, you were showing this to the jury at least for one reason, to show that it wasn't fair to Microsoft that these valuations were this low, and at the end, $242 million was being requested, right?

A. I don't think I ever said fair. I'm saying what are the economic value indicators, and I'm showing those value indicators contemporaneously across time before the patent was issued, after the patent was issued, before the hypothetical negotiation, after the hypothetical negotiation. And so I'm trying to talk about the forces of pressures that would have been present at the hypothetical negotiation, then I compared that to Mr. Reed's opinion. That's what this chart is showing.

Q. Well, I mean, your opinion, Dr. Ugone, is that $242 million is an unreasonable royalty, correct?

A. I will agree with that statement.

Q. So here you're using this to show at least one reason that the $242 million is unreasonable, correct?

A. That's correct.

Q. Okay. Now, you'll agree with me that the time span in this chart is about nine years, correct?
A. Absolutely. We show that at the bottom, from 2001 all the way up to 2006, if that's what you're asking.
Q. Yes. And then the current time period, $242 million is today and that's 2010, correct? That would be nine years, 2001 to 2010?
A. I may not understand your question, but I'll agree with that statement, yes.
Q. Now, let's talk about -- well, let me just ask you this: Is -- is it out of the ordinary for a company to go up in value that kind of multiplier, I guess it's about maybe 20 times or 10 times? Is it -- is it out of the ordinary for a company to go up in value in nine years that much?
A. Well, it's not nine years because you have October 2006 and this data goes through the end of 2009. So what you're asking is is it out of the ordinary to go up this value in three years, and I would say yes, that's extraordinary to do that. That's not a common appearance that you see in the marketplace.
Q. Okay. Well, let's talk about -- let's talk about a couple of years in the life of another company. Let's talk about Microsoft.

A. Sure.
Q. Do you remember when Mr. -- Mr. Pall joined Microsoft, do you remember what he testified to?
A. On the date? I'm not sure I remember. It was about 20 years ago.
Q. He joined in 1990 I believe is what his testimony said. And so Mr. Pall joined in 1990.
Do you know what the stock price was of Microsoft stock in 1990?
A. I don't know that I could give you an estimate of that.
Q. Okay. Well, I looked it up last night. I actually -- I went to Google and I looked it up and got a little chart. It's really kind of nifty what you can get on the Internet.
A. Sure.
Q. And I got this chart and in 1990, the stock price was $1.09. Do you have any reason to disagree with that?
A. No. I will accept your representation.
Q. Okay. And generally it appears that in 1995 and 1996, it was maybe 4 or $5. Do you have any reason to disagree with that?
A. No.
Q. Okay. Now, would you be surprised to hear what

it is in 1990, sir? 1999. I apologize.
A. 1999. No. And I -- and I know it's going to be substantially higher.
Q. Yeah, it's $50 or $49.27.
MR. CASSADY: Could you go ahead and put the next slide up, Mr. Moreno?
Q. (By Mr. Cassady) So in 1990, Microsoft stock was valued at $1.09, but in 1999 it was valued at $50.
A. Yeah. They have to have a functioning product, and they're selling operating systems and they're innovative. And the market is accepting their products, so that's why we see that.
Q. Okay. So -- so you're saying that it was fair for Microsoft's valuation to go up that much but it's not fair for VirnetX; is that true?
A. Again, you keep using this term fair, and I like to look at things from an economic perspective. And yes, you have economic indicators where they come out with innovative products. The market's accepted XP, the market's accepted later products. They've come out with Word; they've come out with Excel; they've come out with PowerPoint. Those are all hugely successive products, and the market rewards a company that puts out hugely successive products and that's why you see this.
Q. And that's not really the question I asked,

Dr. Ugone. What I'm asking you is -- I guess I'll use your term -- is it unreasonable for a company's valuation to go from $1 to $50 in less than nine years?

A. I didn't say it was unreasonable. I said it was extraordinary. It's not a common occurrence. That's what my testimony was.

Q. Okay.

MR. CASSADY: That's all I have.

Thank you, Your Honor.

THE COURT: Thank you. Redirect?

MR. SAYLES: May it please the Court.

REDIRECT EXAMINATION

BY MR. SAYLES:

Q. A few moments ago you said that you thought the valuations that you were shown, including CSMG, were not applicable in this case. Would you explain to the ladies why that is so?

A. There's different ways of doing valuations. There's all the ones that I showed you and those all have a consistent methodology and were roughly in the $15 million range.

Another way to do it is say, well, let me make a projection as to what my sales are going to be.

Now remember, SAIC with its technology and VirnetX have never had a product that they've been able to sell out in the marketplace. But if you say let me forget about that and just project sales and look at those profits and then look at the value of that, that's another way to do the methodology. But that's also a very risky -- a risky analysis because there is no product yet.

But underlying those numbers that I was being shown on cross-examination where huge projections of sales that when you do -- this is fancy term -- net present value, that's looking at the value today versus over time. But they have these huge sales projections of hundreds of millions of dollars in just a matter of two or three or four years.

And SAIC quickly realized that that wasn't going to take place, and they've retracted from those values and they started agreeing with what all these other third parties were telling them, the venture capitalists and everybody else.

Q. And you were asked some questions about the rise in the Microsoft stock price and asked in some way to compare that to VirnetX. Is that a reasonable and fair comparison from an economic standpoint?

A. And I was attempting to say no there. I was trying to give the jury some indication of Microsoft's success in terms of the market acceptance of their products. And as we know in the stock market, the stock market rewards successful companies. Microsoft has had very good products over time: Excel, Word, the operating systems.

VirnetX, there hasn't been any market reward because they haven't even developed a product. They finally had a beta version after the nine years. My understanding is they've achieved no revenues from any sales or licensing of that product.

MR. SAYLES: Pass the witness.

THE COURT: Recross.

MR. CASSADY: No further questions, Your Honor.

THE COURT: All right. Thank you. You may step down.

All right. Who will be your next witness?

MR. POWERS: We will have two final video depositions, Your Honor. The next one is Dr. Victor Larson who's from VirnetX.

THE COURT: Okay. And do I have the times on that one?

MR. POWERS: They are included in the cumulative times that I gave you before. If you want the exact time for these, I can give you that as well.

THE COURT: They were included in the

other four?

MR. POWERS: Yes.

THE COURT: All right. Very good.

(Video playing.)

QUESTION: Good morning, Dr. Larson.

ANSWER: Good morning.

QUESTION: What is your full name?

ANSWER: Victor J. Larson.

QUESTION: And what is your current job title?

ANSWER: I believe it's the Director of Research and Development.

QUESTION: And you're employed by VirnetX?

ANSWER: Yes, I am.

QUESTION: And you believed at the time that a NetEraser client solution would provide many functional advantages over browsers communicating through https?

ANSWER: I believe that the NetEraser product would provide additional benefits to the end user, yes.

QUESTION: Dr. Larson, do you have Exhibit 231 in front of you?

ANSWER: Yes, I do.

QUESTION: And you see this is an e-mail

from you to Bob Short on November 8th, 2005?
ANSWER: Yes, I see that that's what it is.
QUESTION: And you see in the e-mail you write to Dr. Short and say, I did not come away from the Thursday/Friday meetings with a strong feeling that our patent provided any amount of protection against reasonably secure approaches for SIP (i.e. TLS)?
Do you see that?
ANSWER: Yes, I see that.
QUESTION: You see in the second paragraph you say, It seems like if LCS is doing secure SIP between servers, we have nothing to add.
Do you see that line?
ANSWER: Yes, I do.
QUESTION: LCS refers to Live Communication Server; is that right?
ANSWER: I believe that's what it refers to, yes.
QUESTION: And Exhibit 231 reflects your thoughts after the meeting, that if LCS was doing Secure SIP, that VirnetX had nothing to add in terms of security technology; is that right?
ANSWER: Again, this was a -- this was a reaction without looking at Secure SIP in detail or

looking at LCS in detail or looking at our patents in detail.

QUESTION: So then Exhibit 231 reflects your reaction without having looked at your patents yet?

ANSWER: Yes.

QUESTION: Exhibit 231 reflects your reaction to the long meetings with Kendall Larsen, Gif Munger, and other persons, that your patents, as you remembered them, didn't provide any protection against SIP using TLS?

ANSWER: Well, again, I was -- I was representing a feeling without going in and reviewing the -- the -- the patents and -- and secure SIP.

QUESTION: I just asked, based on what you've reviewed on Secure SIP on your patents, have you changed your mind about the strong feeling you had that your patent provided no amount of protection against Secure SIP using TLS as reflected in Exhibit 231?

ANSWER: I -- no. No, I haven't changed my mind.

QUESTION: Have you done any investigation as to whether the VirnetX prototype would infringe any other company's intellectual property?

ANSWER: No, I haven't done that investigation.

QUESTION: Why haven't you done an analysis of whether the Gabriel prototype infringes every patent cited against yours?

ANSWER: I haven't been directed to do that.

QUESTION: It didn't make sense for you to do that on your own without direction?

ANSWER: No. I -- it didn't make sense to me.

QUESTION: You've been handed what is marked as Exhibit 240. It's an e-mail from you to Gordon Warren and others with Bates Number VNET00247657.

Do you recognize this e-mail?

ANSWER: This would have been consistent with something I sent at the time.

QUESTION: Who is Gordon Warren?

ANSWER: He's a developer on the R&D team.

QUESTION: In this e-mail, Exhibit 240, the Subject is Fileshare Registry Change.

Do you see that?

ANSWER: Yes.

QUESTION: What is Fileshare?

ANSWER: Gordon was developing an application to enable sharing files as part of the Gabriel prototype.

QUESTION: In the e-mail Gordon is telling you, group shmoop. It's all vapor ware.

Do you see that?

ANSWER: Yes.

QUESTION: Why is Gordon Warren telling you that it's all vapor ware?

ANSWER: I'm sure Gordon was attempting at some humor here. My guess is he was also expressing that he didn't want to wait to solve this problem until Bob had the group concept flushed out and implemented.

QUESTION: And with humor is Gordon telling you that he believed that Bob Short's group idea was vapor ware?

ANSWER: I think he was just saying that he didn't want to wait for Bob to implement.

QUESTION: What is vapor ware, in your understanding?

ANSWER: It's software that doesn't exist yet.

QUESTION: It's also software that's not likely to exist?

ANSWER: No, I don't -- I don't -- I don't use the term that way. You'd have to ask Gordon if he was using the term that way.

QUESTION: So the log-in box that's on the

page ending in Bates No. 509 was the special log-in for VirnetX users who you were authorizing to access the registry; is that right?
ANSWER: Who were -- this is the log-in to get to the website that contained the registry code, and we -- we put that log-in just so that only users that we had provided the user name and password to would -- would be able to do that.
QUESTION: What users did you provide the user name and password to? Who? Who was provided the user name and password?
ANSWER: Well, all the members of the R&D team and Gif Munger, and I believe it was provided to -- to Kendall Larsen and -- and Sameer.
QUESTION: Do you know whether any of those users ever logged in through this log-in screen?
ANSWER: The -- the members of the R&D team would have logged in multiple times as part of testing and developing the software, and Gif Munger would have logged in multiple times. I -- I don't have knowledge of whether or how often Sameer and Kendall would have logged in.
QUESTION: You can see that the user name -- who chose the user name for this log-in screen, VirnetX?

ANSWER: It was likely me, but I am not for sure.

QUESTION: Did you also choose the password, MS4$2009, question mark?

ANSWER: I may have chosen that, yes.

QUESTION: Is it your recollection that you chose that password?

ANSWER: It -- it is my recollection that I chose that password, yes.

QUESTION: Does your password stand for Microsoft four money 2009?

ANSWER: Yes, that's my recollection.

QUESTION: Why do you have a password that's a question, Microsoft four money 2009?

ANSWER: At that time that was my perception of when the -- based on what people had -- at that time that was my perception of when a -- a trial might occur?

QUESTION: Why did you make that the log-in and password for the VirnetX prototype?

ANSWER: I -- I think I thought it was a interesting password, and I probably copied the password from one place to another place. And so I don't think the -- using it in this context was a -- was a purposeful decision.

QUESTION: Where else have you used the password Microsoft four money 2009?

ANSWER: I have several passwords that I use. I believe I used this password when setting up some log-in accounts for a couple of other developers and then communicated it with them, and then in most cases, they likely changed it to their own password.

(End of video clip.)

MR. POWERS: Our final witness, Your Honor, will be Mr. Kendall Larsen, the President and CEO and Chairman of VirnetX.

THE COURT: All right. Mr. Kendall Larsen.

(Video playing.)

QUESTION: All right. If I understand this, you are the Chief Executive Officer of VirnetX; is that right?

ANSWER: That is right.

QUESTION: Do you hold any other titles with VirnetX?

ANSWER: Yes, I do.

QUESTION: What are they?

ANSWER: Chairman of the Board and President.

QUESTION: When was VirnetX founded?

10:25 ANSWER: VirnetX was founded in September of 2004.
10:25 QUESTION: How many shares do you hold in VirnetX?
10:26 ANSWER: Approximately 8.2 million shares.
10:26 QUESTION: Are you the single largest shareholder of VirnetX stock?
10:26 ANSWER: Yes, I am.
10:26 QUESTION: What's your percentage holdings?
10:26 ANSWER: My individual holdings represent about 20 percent of the company's outstanding common stock.
10:26 QUESTION: Let's take a look at Exhibit 147. Do you recognize Exhibit 147 as Work Order Number 1 as executed between VirnetX on the one hand and Magenic Technologies on the other?
10:27 ANSWER: Yes, I do.
10:27 QUESTION: And did you execute this on or around February 27, 2006?
10:27 ANSWER: Yes, I did.
10:27 QUESTION: Now, following the entry by Magenic and Kendall Larsen, yourself, on behalf of VirnetX in this agreement, did Magenic begin work to
10:28 implement the project goal and the deliverables that are

outlined on page 2 of this work order?

ANSWER: Yes.

QUESTION: So as of February 23rd, 2006, your understanding was that the Live Communications Server, Office Communicator, did not include RFC 3263 as a means for securing communications?

ANSWER: That's correct. We wouldn't have put it in the work order to build products functionally similar to that had we believed it already to be there.

QUESTION: And in connection with the Magenic work on the project, I take it that Magenic reviewed the '135 patent; is that right?

ANSWER: They were given direction by Gif Munger and Sameer Mathur as to implementing those functions that are described in the '135 patent. This is product development.

QUESTION: And was one of the objectives of the work that was being done here was to take the Live Communications Server 2005 and embed in it or develop into it the technologies that are -- among others, that are found in the '135 patents?

ANSWER: In part, yes.

QUESTION: Now, in connection with the work that Magenic was doing on this project to embed the '135 patented technology into the Live Communication

Server, Microsoft product, how long did Magenic work on that?

ANSWER: I would say roughly six months.

QUESTION: Let me show you Exhibit 111. This appears to be a letter from Microsoft to SAIC on the subject of the '135 patent. Have you seen this letter before?

ANSWER: Yes, I have.

QUESTION: And did you see this letter in or around the September 2006 time frame?

ANSWER: Yes, I did.

QUESTION: You'll note in the second to last paragraph Microsoft says that they agree that a meeting might be appropriate. Do you see that?

ANSWER: Yes, I do.

QUESTION: I'm asking, between September of 2006 and February of 2007, did you make any effort to set up a meeting with Microsoft to discuss the subject matter of this letter?

ANSWER: No.

QUESTION: Do you know one way or the other whether Ms. Bumann undertook some efforts?

ANSWER: I can't speak for Ms. Bumann.

QUESTION: Now, in Exhibit 111, Microsoft asked Ms. Bumann for a claim chart to support the allegations that the implementations of RFC 3263 infringe the '135 patent. Do you see that?

ANSWER: I see that, yes.

QUESTION: To your knowledge, did Ms. Bumann send such a claim chart to Microsoft?

ANSWER: Sorry. I'm not aware.

QUESTION: Did VirnetX send such claim charts to Microsoft?

ANSWER: No, we did not.

QUESTION: And in light of that, was one of the goals of the Gabriel technology to embody the patent methods to support litigation?

ANSWER: Yes, it was.

QUESTION: Did you perform an analysis of whether most implementations under RFC 3263 would practice the VirnetX patents?

ANSWER: No.

QUESTION: Is it your belief that any product that has the general functions and benefits of what's described in RFC 3263 necessarily comes under the VirnetX patents?

ANSWER: No.

QUESTION: How long after December of 2005 did VirnetX continue to work with Microsoft software to attempt to introduce instant secure connect, or Gabriel technology?

ANSWER: We continued all the way through 2006. So we continued working. We let SAIC know that they needed to contact Microsoft per the contract.

And, you know, I'm talking a month or two here. It could have been November where we had that conversation and the notice came in December, but it was in the fourth quarter of the architectural design document when that took place.

We were not stopped by that process, and we said we're going to continue because we think that there's a way to work this out, work together. And we said the best way to work that out would be hire Magenic, which was their top developer. And if there was anyone who could help us integrate our invention with Microsoft platforms, it would be Magenic. So it was really a well-intended effort.

QUESTION: One of Magenic's -- Magenic's objectives in attempting to modify Microsoft's products was the goal of utilizing VirnetX's patented technology in Microsoft's products, right?

ANSWER: That's correct.

QUESTION: And so VirnetX spent the lion's share of its Series A financing in this effort in 2006 to modify Microsoft's products to practice the claims of the patents, right?

ANSWER: To build a product that we felt completely would practice a full implementation of our -- of our patents, yes. And we believed that Microsoft implemented a portion of that along the way, and it was an increasing portion throughout the development process.

QUESTION: Isn't it true that you figured out what Microsoft was doing in terms of implementing SIP in the summer of 2006?

ANSWER: Yes.

QUESTION: It's your belief, and was in the summer of 2006, that Microsoft was not actually practicing RFC 3263, right?

ANSWER: Yes.

QUESTION: And when SAIC gave notice to Microsoft that Microsoft was potentially infringing the VirnetX's intellectual property, Microsoft was told that if it were practicing RFC 3263, it was potentially infringing, right?

ANSWER: It was a misstatement. Yes, I do remember that. And it was a notice from Pam Bumann. It was a general indicator that they were practicing 3263 and if they were -- and Microsoft said: We're not.

QUESTION: To your knowledge, SAIC never

sent Microsoft a claim chart, charting any implementation of RFC 3263 against the '135 patent, right?

ANSWER: My answer is no.

QUESTION: Who, if anyone, at SAIC or VirnetX contacted Microsoft to set up a meeting after SAIC received this letter?

ANSWER: Pam Bumann.

QUESTION: When did Pam Bumann contact Microsoft to set up a meeting?

ANSWER: After September 12, 2006.

QUESTION: When?

ANSWER: You'd have to ask her specifically. But it was a -- a -- an action that we were trying to wait for a response, wait for a meeting date. I was ready to go, and there was never a response from Microsoft to set the meeting up.

QUESTION: A response to an inquiry made by Pam Bumann?

ANSWER: Yes. In other words, this meeting request was in theory. In practice, they never returned the calls.

QUESTION: But in your discussions with Pam Bumann, she never told you that she'd actually sent Microsoft a claim chart or any other evidence to substantiate SAIC's claim that an implementation of RFC 3263 could infringe the '135 patent?

ANSWER: That's correct. The answer is yes.

QUESTION: To your knowledge, did SAIC ever provide Microsoft with claim charts or other evidence that any Microsoft product infringed claims of the VirnetX patents?

ANSWER: To my knowledge, no.

QUESTION: Does VirnetX have a view, one way or the other, on which would be more valuable to a potential licensee? Licensing the specific technology in an SDK versus licensing patent rights to practice it a different way?

ANSWER: We believe them equally balanced as far as their value to the end user, whether they wanted to implement it in our object code or whether they wanted to write their own object code.

QUESTION: You believe the two types of licenses would carry similar values to the potential licensee?

ANSWER: Yes.

QUESTION: Would you agree that as a general matter, a company with significant resources, like a Google or a Microsoft, would be able to develop

10:39 the technology contained in the software development kits on its own and apart from VirnetX for around $5 million?

10:39 ANSWER: I would say that our development of Gabriel was in that range, and so I think that a company of Microsoft or Google's stature could develop the technology for that, yes.

10:40 (End of video clip.)

10:40 MR. POWERS: Your Honor, that completes the witnesses in Microsoft's case.

10:40 And we'd like to hand up a list of the illustrative exhibits that have been admitted throughout the course of the trial similar to the substantive exhibits.

10:40 THE COURT: All right. Very well.

10:40 Any objection to the illustrative exhibits?

10:40 MR. McLEROY: No, Your Honor.

10:40 THE COURT: Okay. Be admitted.

10:40 Does Microsoft rest?

10:40 MR. POWERS: Yes, Your Honor.

10:40 THE COURT: All right. Rebuttal.

10:40 MR. McLEROY: Yes, Your Honor. VirnetX calls Professor Mark Jones back to the witness stand.

10:40 THE COURT: Professor Jones.

MR. McLEROY: Your Honor, may I approach?
THE COURT: Yes.

MARK JONES, PLAINTIFF'S WITNESS, PREVIOUSLY SWORN

DIRECT EXAMINATION

BY MR. McLEROY:

Q. Good morning, Professor Jones.
A. Good morning, sir.
Q. Now, last week Mr. Caldwell asked you questions about the infringement of the VirnetX patents. You understand that I am now going to cover the validity of the VirnetX patents with you?
A. Yes, sir.
Q. All right. Now the '135 patent was granted in I think in 2003 and the '180 patent was granted in 2007. What is the effect of granting a U.S. patent?
A. Well, as Judge Davis has told us, when the United States Patent and Trade Office grants a patent, that we are to presume that it is valid.
Q. And let me ask you right off the bat. Do you agree or disagree with Dr. Wicker's opinions that the '135 patent and '180 patents are invalid?
A. I disagree with that. None of the references Aventail DVPN or Windows NT anticipate or render obvious the VirnetX patents.
Q. Now, last time -- last week when you were on

the witness stand, I think your testimony lasted for more than three hours. Are you going to be here that long again today?

A. No, sir. Today I'm going to be testifying -- testifying about the validity of the patents, and to show a patent is valid, I need to show that at least one element is missing from the prior art that is in the patents.

Q. Can you give me example of what you mean?

A. Well, let's say that patents had elements A, B, and C in a claim and the prior art had just elements A and B but not C, then the patent would be valid.

Q. So let's see if we can get an example from this case. Is what you're saying, Professor Jones, that if the jury finds that -- that just one thing is missing from, say, Windows NT 4, that then Windows NT 4 would not anticipate the VirnetX patents?

A. That's correct. I mean, it makes sense if -- if you have an invention, all right, and if the prior art is missing part of that invention, then they don't have an invention.

Q. Well, Professor Jones, I know you'd probably like to discuss your entire validity case today, but because all that's required is to show that one element is missing, I'm going to ask you just to focus on one

element with respect to the prior art. Is that okay?
A. Yes, sir.
Q. Start with Windows NT 4. Is Windows NT 4 the same as the VirnetX patents?
A. No, sir, it's not.
Q. Well, what is the biggest difference between Windows NT 4 and the VirnetX patents?
A. Well, I think to -- to illustrate that I would like to put up Claim 1 of the '135 patent.
MR. McLEROY: Your Honor, may I approach the easel?
THE COURT: Yes, you may.
Q. (By Mr. McLeroy) Can you see that, Dr. Jones?
A. Yes, sir.
Q. Which part of this claim should we focus on?
A. I'd like to focus on for this important difference on the second step of that, and it's my opinion that Microsoft Windows NT does not determine whether the DNS request transmitted in step 1 is requesting access to a secure website.
Q. And, Professor Jones, what evidence confirms for you that Windows NT 4 does not meet that second step of this claim?
A. The evidence I reviewed in the case included source code, but I think it would be helpful to show

Mr. Pall's testimony from -- from last week on that topic.

MR. McLEROY: Can we set up the first slide?

Q. (By Mr. McLeroy) Is this the testimony you're referring to?

A. Yes, sir, it is. So -- so Mr. Pall was asked: So isn't it true, don't you agree, Mr. Pall, that the system you're demonstrating is not determining whether the VPN DNS request transmitted is requesting access to a secure website?

Q. And his answer was: The system is not determining that specifically, sir.

Is that right?

A. Yes, sir.

Q. Now, was Mr. Pall's testimony correct on this question?

A. Yes, sir. And I think we all saw the demonstration of Windows NT with the three computers up here on a table and -- and one computer beneath the desk.

In that demonstration, we saw that the VPN was connected and set up regardless of whether it was typed in www.securewebsite.com or whether it was www.eBay.com. There wasn't a determining, there was

just a setting up.
Q. One other topic related to Windows NT 4 --
MR. McLEROY: And, Your Honor, may I approach the easel again?
THE COURT: Yes, you may.
Q. (By Mr. McLeroy) This is the illustration that Dr. Wicker gave of the Windows NT 4 system, is that right, Professor Jones?
A. Yes, sir.
Q. Did Windows NT 4 operate in the manner that Dr. Wicker described here?
A. No, sir, it did not.
Q. Let me ask you a more basic question. Does this diagram appear anywhere in any of the evidence that you have seen in this case describing Windows NT 4?
A. No, sir, it does not.
Q. Okay. Did you find anything even close to this diagram in the evidence?
A. No, I didn't find anything close, but I did find a diagram in his report that -- or -- sorry -- in Microsoft evidence that was similar to part of this diagram.
MR. McLEROY: Could you put up Defendant's Exhibit 3064?
Q. (By Mr. McLeroy) All right. Professor Jones,

you have it there on your screen, don't you?
A. Yes, sir.
Q. What is Defendant's Exhibit 3064?
A. This is a document that Microsoft wrote to describe the VPN technology in Windows NT.
MR. McLEROY: Could we turn to page 22? And please blow up the diagram and the text underneath the diagram at the top of the page.
Q. (By Mr. McLeroy) Professor Jones, is this the diagram that you're referring to?
A. Yes, it is.
Q. Are their differences between the actual Microsoft diagram and then the illustration that Dr. Wicker gave here in court?
A. Yes, there are. For example, when we're looking at the diagram up here on the board, it shows a secure DNS request going from the client to the tunnel client.
Q. Let me stop you there. This is where Dr. Wicker wrote secure DNS request and then he shows an arrow from the first computer to the second computer. Is that what you're referring to?
A. Yes, sir.
Q. Now, what did the actual Microsoft document show happens between those two computers?

A. The Microsoft document shows that there's a phone call going from the dial-up client to the tunnel client in this case.

Q. So the first computer makes a phone call to the second computer; is that right?

A. Yes, sir. It uses what's called -- a piece of hardware called a modem to make that call.

Q. How do you know it's a phone call that goes from the first computer to the second computer?

A. Well, a couple of things in this diagram as well as the rest of the document. First, I see that the client in the far left is called the dial-up client.

Q. Okay. So in the actual Microsoft document, it's called the dial-up client, right?

A. Yes, sir.

Q. Now, is that referring to what Dr. Wicker just called a client?

A. I believe it is.

Q. So he left off the words dial-up?

A. Yes, sir.

Q. Okay. You said a couple of things. Was there something else you wanted to point to?

A. Well, when we look at the highlighted text below the figure, note that it says, The client computer places a dial-up call.

That's an indication that a phone call using a modem is being made.

Q. Professor Jones, is it possible that there's some confusion here, that a telephone call is the same thing as a secure DNS request?

A. No, sir. There's -- a secure DNS request is not a phone call.

Q. And, Professor Jones, is there any evidence that the Windows NT 4 system is able to make a determination based on a secure DNS request, as we see in Dr. Wicker's illustration?

A. No, sir.

Q. Let's talk about DVPN now. Is DVPN the same as the VirnetX patents?

A. No, sir, it's not. I found several differences. And further, this DVPN was developed, as we've heard in testimony, to solve a different problem.

Q. Well, what was the single most important difference between DVPN and the VirnetX patents?

A. Well, I think the most important difference was like Windows NT, DVPN was not doing a determination based on a DNS request to go on and then initiate a VPN.

Q. Didn't Dr. Wicker testify that DVPN did make a determination based on a DNS request?

A. Yes, sir, he did.

Q. Well, when the jury has to figure out if DVPN -- DVPN did or did not make that determination, what evidence should they rely on? What evidence should they look at?

A. I think, for example, we've heard testimony last week from Mr. Saydjari indicating that he's the person who funded DVPN, that he doubted that DVPN had -- was DNS-triggered. But I think the best place to look is in the source code for DVPN.

MR. McLEROY: Could you pull up Plaintiff's Exhibit 985, and turn to the eighth page when you have it? And actually there's a section at the bottom I'd like you to highlight so we can all see it.

Q. (By Mr. McLeroy) Is this the source code that you're referring to, Professor Jones?

A. Yes, sir. This is the source code that Dr. Wicker cites to support his contention that there is a determination in DVPN based on DNS request.

Q. What does this source code indicate to you?

A. This source code is discussing and looking at IP addresses. So if we see in this example IP underscore ADDR, remember, IP addresses are like what we see on the far right of the screen. If I can -- like 127.0.0.1 is an example of an IP address as opposed to a domain name which might be something like www.Yahoo.com.

Q. Now, to be real clear, does this source code that we're looking at on the screen, does it reference a DNS request at all?

A. No, sir, it's not.

Q. Finally let's turn to Aventail. Is Aventail the same as the VirnetX patents?

A. No, sir.

Q. Well, what is the biggest difference between Aventail and the VirnetX patents?

A. The biggest difference is that Aventail does not use or create a VPN.

Q. Well, Professor Jones, I know in the Aventail manual that Dr. Wicker showed us last week it used the term VPN. Is that enough? Does that -- does that satisfy a VPN element of the claim?

A. No, sir, it's not just enough to use the words VPN. That's why Judge Davis has given us a construction to use, and we are to compare that construction for VPN to what's actually going on in the products, not just look at words.

MR. McLEROY: Would you put the next slide up for presentation?

Q. (By Mr. McLeroy) Is this that definition that you're referring to?

A. Yes, sir. It states that a virtual private network is a network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.

Q. What about this definition indicates to you that Aventail does not form a VPN?

A. I would -- I would focus in this case on the second word, network. Aventail forms a point-to-point connection, a SOCKS connection. It doesn't create a network or a VPN.

Q. Well, what's the difference between a point-to-point connection and a network or virtual private network?

A. Well, sir, a point-to-point connection is -- is a connection that you put something -- it's like a garden hose, you put something in one side of that garden hose and it will come out the other. Unlike a network where I can typically address packets or messages and have them delivered to different computers. One mechanism for doing that is routing.

Q. All right. Let me ask you a first question about this. Do you know if Dr. Wicker agrees or disagrees with you that a -- that Aventail creates a point-to-point connection?

A. Dr. Wicker agrees that Aventail creates a point-to-point connection. I see this when I look at

Dr. Wicker's testimony. He discusses Aventail using a SOCKS -- SOCKS connections. Further in his deposition he indicates that he believes that SOCKS creates point-to-point connections.

MR. McLEROY: Can we go to the next slide?

Q. (By Mr. Cassady) Is this that deposition testimony of Dr. Wicker that you're referring to?

A. Yes, sir. And he's being asked about whether SOCKS is a point-to-point connection, and going to the bottom indicates that he's pretty sure it has to be point-to-point.

Q. Now I guess that doesn't quite take us all the way there. Have we heard any testimony so far in this case about whether a point-to-point connection is or is not a VPN?

A. Yes, sir. For example, the testimony of Mr. Pall last week.

Q. All right.

MR. McLEROY: Could you go to the next slide?

Q. (By Mr. McLeroy) What was Mr. Pall's testimony?

A. Here he was asked: And you agree that, therefore, a VPN is more than just a point-to-point connection?

And he answers: Yes, sir.

Q. Do you agree with Mr. Pall on this issue?
A. Yes, sir, I do.
Q. Well, that covers the '135 patent. Let's talk about the '180 patent.
What is the biggest difference between the '180 patent and all of the prior art that Microsoft has discussed in this case?
A. It's the -- it's the -- the patents have the secure domain name elements and the secure domain name service elements that aren't there in the prior art.
Q. Well, if the prior art doesn't use secure domain names or secure domain name services, what do they use?
A. The use conventional domain names and conventional domain name services. And these things have been around for years.
MR. McLEROY: Would you go to the next slide, please?
Q. (By Mr. McLeroy) Here is Judge Davis's construction of secure domain name.
Do conventional domain names satisfy the judge's definition?
A. No, sir, they don't. Because they don't correspond to a secure computer network address as required in this claim construction.

Q. A few wrap-up questions, Professor Jones.
What is the role of hindsight in an obviousness analysis?
A. Hindsight should not play a part in obviousness analysis. Hindsight would be something like using the patent as a recipe of things to do and then go looking at prior art references for pieces and parts and words, assembling them altogether and then saying that that renders obvious or -- or the -- the patents. That would be the incorrect path to take.
Q. Well, if hindsight is the wrong way to do it, what is the right way to do an obviousness analysis?
A. The right way to do it is to put yourself in the shoes of one of ordinary skill in the art at the time of the invention, in this case late '99, early 2000. Look at the information before you, including these prior art references, and ask whether or not it would have been obvious to create the invention using those references.
Q. Well, let me ask you that exact question. Were the '135 patent and '180 patents obvious in the year 2000 when the patent applications were filed?
A. No, sir, they were not.
Q. Professor Jones, to wrap up once and for all, can you tell the jury what your opinion is on the

10:57 validity of the '135 and '180 patents?
10:57 A. Yes, sir. None of the three prior art references -- Aventail, DVPN or Windows NT 4 -- anticipate or render obvious the VirnetX patents. The '135 and '180 patents are valid.
10:57 Q. Thank you.
10:57 MR. McLEROY: I pass the witness, Your Honor.
10:57 THE COURT: Cross-examination.
10:58 MR. POWERS: May I approach, Your Honor?
10:58 THE COURT: Yes, you may.
10:58 MR. POWERS: May I proceed, Your Honor?
10:58 THE COURT: Yes, you may.

CROSS-EXAMINATION

10:58 BY MR. POWERS:
10:58 Q. Good morning still, Dr. Jones.
10:58 A. Good morning, sir.
10:59 Q. You began your discussion with the presumption of validity. Do you recall that on direct examination?
10:59 A. Yes, sir, I do.
10:59 Q. Now, the presumption of validity doesn't mean that the jury can't find the patents invalid, does it?
10:59 A. It does not mean that, that's correct, sir.
10:59 Q. In fact, juries do that all the time, don't they?

A. I believe they can, yes, sir.
Q. So in this case, the Patent Office did not actually consider any of the three pieces of prior art we discussed: Aventail, DVPN, or PPTP NT 4.
A. Yes, sir. They were not explicitly on that list.
Q. So there's no presumption that the Patent Office looked at those pieces of prior art and decided that VirnetX's patents were valid over those prior art, is there? They just -- they didn't even look at it at all.
A. That would be what -- the record indicates they did not, so we aren't to presume that they did.
Q. This jury would be the first opportunity to decide whether the VirnetX patents are valid over those pieces of prior art, true?
A. I believe that's correct, sir.
Q. Now, the Patent Office also didn't have the VirnetX source code or technical documentation, did it?
A. Not that I'm aware of, sir.
Q. And, in fact, the Patent Office doesn't make a technical evaluation of whether their source code or product is any good, does it? That's not the Patent Office's job.
A. That's correct, sir.

Q. Now, let's turn first to your discussion of the Windows prior art, which is PPTP and AutoDial.
Do you recall that?
A. Yes.
Q. You did not dispute in your testimony that PPTP is an easy and automatic way of setting up a VPN, did you?
A. I didn't say anything about that, sir.
Q. And the argument that you did make on direct is that you believe that the determining step in the '135 patent was not satisfied by the PPTP/AutoDial prior art, right?
A. Yes, sir.
Q. Now, you cited, for example, the testimony of Mr. Pall when he was being cross-examined by VirnetX's lawyer, right?
A. Yes, sir.
Q. And that testimony came up in the context of Mr. Pall's carrying out the demonstration that VirnetX's lawyer asked him to carry out, right?
A. Yes, sir.
Q. And what VirnetX's lawyer asked him to do was to type in a fake, bogus name, right?
A. I believe in one case, it was eBay, and in another case, it was a made-up name, yes, sir.

Q. It was thisisnotasecurewebsite.com, right?
A. Something like that, yes, sir.
Q. That's not a real website, is it?
A. Not that I'm aware of.
Q. Okay. And in that context, that was the context in which Mr. Pall said there was no determining being done with the fake, bogus name, right?
A. I believe he was asked about the system, sir. I'm not sure what was in his head.
Q. But it was after the discussion of that fake, bogus demonstration, right?
A. Yes, sir.
Q. All right. Now, on the demonstration that Mr. Pall gave with a real domain name, it did determine a name, didn't it?
A. No, sir.
Q. In fact, what happened in that demonstration is Mr. Pall typed in a genuine address, and it went to the AutoDial address book, right? That's how it works.
A. I would not describe it that way, sir, no, sir.
Q. Well, it -- you did see the AutoDial address book pop up on the screen.
A. I don't recall if I saw it pop up on the screen, but I'm familiar with how it works.
Q. You were here during the testimony?

A. Yes, sir.
Q. Okay. And you don't dispute that the AutoDial address book came up on the screen.
A. I believe he had it up on the screen. I don't remember if it came up during that process or not.
Q. You had an opportunity to inspect that system for two full hours before it was shown to the jury, didn't you?
A. Yes, sir.
Q. So you know that the AutoDial address book contains addresses of websites that have been visited.
A. By addresses, you mean like IP address, sir, or --
Q. No. The path by which it was going to reach that -- or create that VPN.
A. I believe it contains the IP address and an indication of whether it's going to use PPTP, yes, sir.
Q. Exactly. The AutoDial address book says it's going to use PPTP for a particular secure connection, doesn't it?
A. That's the phone book, sir.
Q. Yes or no, does AutoDial do that? You just said it did.
A. No, sir, I didn't. Could you repeat the question, please.

Q. You just said that it contains an indication that it will use PPTP to make the connection.
A. The phone book --
Q. That's true, isn't it?
A. The phone book does, yes, sir.
Q. Okay. Now, let's turn then to -- well, let's stay with that demonstration for a moment.
You were here when VirnetX's lawyer cross-examined Mr. Pall and made him get down on his hands and knees and look at a Windows 2000 sticker that was on the bottom of the box?
A. Yes, sir.
Q. And he made the point that the Windows 2000 software came out in 2000.
Do you recall that?
A. Yes, sir.
Q. Now, you know that the software running on that machine that was demonstrated was not Windows 2000 software. You know that it was a 1996 NT software, don't you?
A. On that machine, sir? Yes, sir. That was Windows NT 4, I believe, yes, sir.
Q. Which is 1996.
A. That is my recollection, yes, sir.
Q. And that showed up actually on the screen when

you went to go inspect the demonstration, didn't it?
A. It may have, but I would agree that that was Windows NT 4 software from that timeframe, yes, sir.
Q. And that timeframe was 1996.
A. I believe so, yes, sir.
Q. So we didn't need to get down on our hands and knees and look at an old sticker to find out what software was running; it's right on the screen, and it says '96, didn't it?
A. On that computer, yes, sir.
Q. All right. Now, you haven't here offered an opinion as to whether any later versions of the BIOS would affect the operation of that 1996 software, did you?
A. I have not offered an opinion on that, sir.
Q. Let's turn to the DVPN software for a moment.
Do you recall testifying that in that one, there was no determining step as well?
A. No determination made an element as for the '135 patent, yes, sir.
Q. All right. And you based that conclusion on this source code analysis that Dr. Wicker is relieving on. Do you recall that?
A. No. I pointed out an example. My conclusion, though, is based on an analysis of all the source

code -- or the source code in its entirety, as well as the other documents.

Q. Now, let's go to the source code that you showed the jury, and that was in PX985. You asked the jury to look at the bottom of Page 8.

MR. POWERS: So let's bring that up, please, Chris.

Can we dim the lights, please?

Q. (By Mr. Powers) So this is the portion that you showed the jury, and you said what it's looking at is IP addresses, not DNS requests, right?

A. Well, this is the portion that Dr. Wicker showed, and this is what I'm referring to.

Q. All right. And this is what you showed the jury?

A. Yes, sir.

Q. Now, if you go forward two pages in the software --

MR. POWERS: Let's bring up the two pages of Page 10, Chris. And let's highlight DNS, lookup right there towards the top of the page. And then parse_secure about -- oh, almost about five or six lines from the bottom.

Q. (By Mr. Powers) Do you see that?

A. Yes, sir, I do.

Q. Now, this is a section of the code that is talking about DNS lookups, not IP addresses, right?
A. That's correct, sir.
Q. And you didn't show the jury this portion.
A. No, sir, I didn't.
Q. And parse_secure is where a determination step is occurring, isn't it?
A. I don't believe that parse_secure is doing a determination whether to set up a VPN or not. No, sir, it does not do that.
Q. It's your testimony that a VPN is not set up after this parse_secure step?
A. It will -- it's not set up as a result of the parse_secure step, no, sir.
MR. POWERS: Let's go to the very next page, Page 11, of the source code. And, Chris, could you bring up, oh, the first half.
Q. (By Mr. Powers) You didn't show this portion to the jury either, did you?
A. No, sir, I didn't.
Q. And you see about, oh, halfway down where it says count = dns_lookup, that's another DNS lookup in the DVPN code?
A. Yes, sir.
Q. And the parse_secure is right below that as

well?

A. Yes, sir.

Q. And the very next step --

MR. POWERS: Chris, could you scroll down?

Q. (By Mr. Powers) -- is vpn_cache. That's when the VPN is formed, isn't it?

A. I -- I see that. That is not when the VPN is formed, no, sir, it's not.

Q. That is discussing the formation of a VPN, though, isn't it, Dr. Jones?

A. No, sir, that's not what it's doing.

Q. That's your testimony?

A. Yes, sir.

Q. You didn't provide that testimony to the jury on direct, did you, sir?

A. No, sir.

Q. And in fact, this is the portion that Dr. Wicker relied on, isn't it?

A. No, sir. Dr. Wicker pointed to a different portion, the portion I showed.

MR. POWERS: Chris, could you put up PX875, just Page 27, and bring up the middle where it's about Pages 3 -- where it's Steps 3 through 5 -- look at even 3 through 8.

Q. (By Mr. Powers) This is a portion of

Dr. Wicker's report that you read it, right?
A. Yes, sir, I did.
Q. And it's specifically referring to the DVPN source code, right?
A. Yes, sir.
Q. And it's specifically referring to DVPN source code relating to DNS lookups, not IP address, right?
A. It does have DNS lookups, yes, sir.
Q. And you didn't show the jury that or even talk about it, did you?
A. His report? No, sir, I didn't.
Q. All right. Let's turn next to Aventail.
With regard to Aventail, as I heard your position, it's that Aventail is not a VPN because it's a point-to-point network. That was the argument you made?
A. Point-to-point connection, sir, yes, sir.
Q. Point-to-point connection.
Now, the -- let's go to the Court's construction. You put it up. And the Court's construction doesn't say it can't be a point-to-point connection, does its?
A. No. It says it has to be a network, so that precludes a point-to-point connection, sir.
Q. Yours is that a network precludes point-to-point because it has to -- why? Because there

have to be more than two computers?
A. No, sir.
Q. Nothing in Judge Davis' construction says anything about whether there's a point-to-point connection, does it? You'll agree with that?
A. It doesn't mention those words explicitly. That's what a network is, sir.
Q. But it's not in Judge Davis' construction, which is what the jury has to follow, right?
A. I would say it is because of the word network, sir.
Q. Now, in fact, Judge Davis' construction requires that for a VPN to exist, it has to be both data security encryption and anonymity. We talked about that a couple of days ago.
Do you recall that?
A. Yes, sir.
MR. POWERS: Chris, could we bring up the testimony that -- the slide that Dr. Jones used quoting Mr. Pall's trial testimony?
Nope. Mr. Pall's trial testimony, the one from his slide.
Q. (By Mr. Powers) Well, let me just ask you, because I wrote it down.
Mr. Pall testified that a VPN has to be

more than just a point-to-point. That was the testimony you quoted, right?

A. Yes, sir.

Q. And that's exactly what Judge Davis' construction says. It has to be more, because it has to be both anonymous and encrypted, right?

A. I would say that those are two things it has to be, but that is not sufficient.

Q. So Mr. Pall is right in his testimony in saying a point-to-point by itself isn't enough to be a VPN. There has to be more. That's all he said, and that's true, isn't it?

A. I would agree with that.

Q. And two things we know that it has to be under Judge Davis' construction is secure data and anonymous.

A. Data security and anonymity, yes, sir.

Q. All right. Now, you've testified that a point-to-point connection can be a VPN, haven't you?

A. That one could construct such a system, yes, sir.

Q. So a point-to-point connection can be a network.

A. Not when it's simply a point-to-point connection, no, sir. You could use a point-to-point connection to create a network. I would agree with that.

Q. And --

MR. POWERS: Chris, could we bring up Dr. Jones' deposition from December 19, 2008, at Pages 62, Line 15, through 63, 7?

Q. (By Mr. Powers) This was --

MR. POWERS: Let's go back up to -- there's the question.

Q. (By Mr. Powers) This is your testimony in December of 2008, wasn't it, Dr. Jones?

A. Yes, sir.

Q. Question: If you met all the other requirements, we're taking about with an ability to communicate between them and some aspect of addressing or identifying to whom it is destined, then a point --

Answer: I guess by point-to-point, what are you -- I'm not sure what you're saying there.

MR. POWERS: Then let's go to the next question, please, Chris.

Q. (By Mr. Powers) By point-to-point, I am referring to, for example, this network that's on Page 24 of Exhibit 3, where you have a point being the PC on the left and another point being the PC on the right.

And your answer was: You could form a

network using that wire, yes.
Do you see that?
A. Yes, sir.
MR. POWERS: And, Chris, could you bring up the figure that Dr. Jones was discussing in that exact testimony.
Q. (By Mr. Powers) That was a page from the technology tutorial that had been discussed by the parties at that time, right?
A. I don't recall at this point, sir. That's certainly possible.
Q. You recall it being a point-to-point wire connection?
A. I -- I know that we're referring to a wire here, sir. I don't recall the rest of what was being done.
Q. And you agree your testimony said that a point-to-point wire connection can be a network.
A. I -- I agree that's what I testified to, sir.
Q. All right.
A. And I would agree that under certain circumstances, it could, yes, sir.
Q. Now, PPTP, you've already testified, creates a virtual private network, right?
A. Yes, sir.

Q. And PPTP stands for point-to-point, doesn't it?
A. Yes. It uses a point-to-point tunnel to connect the other multiple computers.
Q. All right.
MR. POWERS: Now, could we bring up DX3064, please, at Page 5, Chris?
And can you blow up the portion -- the second from the bottom, second paragraph from the bottom. Actually -- sorry -- the paragraph just above that. It's very small on this. Here we go.
Q. (By Mr. Powers) There it says -- and this is an exhibit from the user's perspective of the VPN as a point-to-point connection between the user's computer and a corporate server.
Do you see that?
A. Yes, sir, I do.
Q. And that's an accurate description, isn't it?
A. I think that's a reasonable description for what they're describing here, yes, sir.
Q. All right. Now let's turn to the '180 patent for a moment.
You testified --
THE COURT: Mr. Powers, you have about three or four minutes left.
MR. POWERS: Thank you, Your Honor.

Q. (By Mr. Powers) You testified that none of the prior art references satisfy the secure domain name requirement because they're just regular domain names, right?

A. Yes, sir.

Q. Now, Judge Davis' construction that the jury has to follow doesn't say that it can't be a regular domain name, right?

A. I believe it does. It says that they have to -- that the domain names must correspond to secure computer network addresses.

Q. And a secure address is one that just requires authority to access, right, under his construction?

A. I believe it has a -- my recollection is, it also requires being capable of DVPN communications.

Q. True. Exactly.

So as long -- and so a regular DNS -- a regular domain name, as long as it corresponds to a secure domain name address, that satisfies Judge Davis' construction, doesn't it?

A. Not -- what you said, sir, is not a possibility. So you've used the words, but that's not an accurate description of what would happen.

Q. Now, you're -- the reason in your expert report that you gave as to why a -- you believe Judge Davis' construction can't be satisfied by a regular domain name is that the domain name has to be designed in order to correspond to a secure website, not just that it, in fact, corresponds to one. That's true, isn't it? That's what you said in your report?

A. That's one way -- being designed to correspond is one way that it can correspond, yes, sir.

Q. But that's not what you said in your deposition or your report. You said that's what you thought it meant to correspond, right?

A. I -- I don't recall whether I used that as an example, sir, or I said that it meant that.

Q. Now, you'll recall that VirnetX argued that claim construction, and Judge Davis did not adopt it. Do you recall that, that it has to be designed limitation. Judge Davis said it merely corresponds. That was his construction, wasn't it?

A. I don't -- I don't believe that there was an argument that it had to be designed, no, sir.

Q. In any event, Judge Davis did not include such a requirement of design into the -- into the construction, did he?

A. I believe that's one way in which it corresponds, so I believe he did by the way he made his construction, sir.

Q. Let's be clear. Judge Davis did not include anything saying that design to be correspond is required, just must correspond; that's fair?
A. He didn't use those exact words, no, sir.
Q. The exact word he used, which is has to correspond, right?
A. That's what -- corresponds, one way to satisfy that is to be designed to be a secure domain name.
Q. And another way to satisfy it would be, if I type in that name, it prints back that secure address, that corresponds then, doesn't it?
A. It does, sir.
Q. It does, or it does not?
A. No, sir.
Q. So if I type in the name of a secure address, and that goes out and brings back that secure address, your testimony to this jury is that that name doesn't correspond to the address?
A. Not -- you'd have to tell me the rest of the system, sir, but just doing that, no, sir, that doesn't meet the elements of the claims.
MR. POWERS: No further questions, Your Honor.
THE COURT: Thank you.
Redirect?

MR. McLEROY: Yes, Your Honor.

REDIRECT EXAMINATION

BY MR. McLEROY:

Q. Professor Jones, I'll start where -- the same place Mr. Powers started with the Windows NT demonstration that we saw in the courtroom here.

Is www.ebay.com, is that a real domain name or a bogus domain name?

A. That's a real domain name that you can go find on the internet.

Q. What happened when Mr. Pall typed in www.ebay.com into the demonstration system?

A. The system set up a VPN.

Q. And what does that indicate to you about whether or not Windows NT 4 makes or does not make a determination to set up or initiate a VPN based on a DNS request?

A. Well, that confirms the understanding I got from looking at the rest of the evidence and the source code for this, that there's not a determination based on a DNS request to set up a VPN in Windows NT.

Q. A little bit more about the demonstration. Mr. Powers referred to the time you spent inspecting the demonstration system before it was shown here in court.

Do you remember that?

A. Yes, sir.
Q. All right. And he focused on what software was running on the computer sitting over there on Microsoft's counsel table; is that right?
A. Yes, sir.
Q. And he was careful not to ask you what software was running on these three computers on this side of the courtroom.
A. Yes, sir.
Q. What software was running on some of the computers on this side of the courtroom?
A. Well, on two of those computers, an early version, a beta version, of Windows 2000 or what became Windows 2000 was running.
Q. Now, turning to DVPN, why did you choose to show the source code up here on the screen that you did?
A. That was the source code that Dr. Wicker cited to in his chart, and it's the source code he showed to the jury, so that was the source code that I discussed, but --
Q. Did you just review that source code, or did you review all the source code in that file in Plaintiff's Exhibit 985 that we saw?
A. Well, I certainly reviewed all the source code in that file, but I also reviewed other files in the

DVPN system to understand what was being put forward.
Q. Does any of the other code, any of the other source code in Plaintiff's 985 or any of the other DVPN source code change your opinion that DVPN does not make determinations based on a DNS request?
A. No, sir. It confirms my opinion of how it works.
Q. All right. Then on Aventail, on the discussion of point-to-point connections, what does PPTP stand for?
A. I believe it's point-to-point tunneling protocol.
Q. Is that the same thing as a point-to-point connection, or is that something different?
A. That's something different. It uses -- PPTP uses a -- what's called a point-to-point tunnel to allow, say, a client computer on one side to communicate with a network of computers on the other.
That client computer can send a packet with -- as it showed, with an IP address in it and have that packet delivered to any of the computers on the private network on the other side of the tunnel.
So it's not -- it's using a point-to-point connection. Many things use a point-to-point connection. It, however, is creating a virtual private network.

Q. So is the PPTP protocol, does that create a garden hose, or does that create something else?
A. That doesn't create a garden hose; that creates a network, sir.
Q. Okay. Now, finally, let's look at the secure domain names. That's a claim term in the '180 patent, right?
A. Yes, sir.
Q. Can you give me an example of what a regular, standard domain name was, you know, something that's been in existence since the '80s?
A. How about the -- if I can go as far back in the '80s in my head, but how about www.yahoo.com as a conventional domain name?
Q. What did the inventors use as examples of secure domain names in their '180 patent?
A. Well, in that they would use something like www.yahoo.scom to -- in that case, indicating that that's for a secure domain name.
Q. What would have happened if you sent a secure domain name to a regular DNS server?
A. You would have gotten back an error that would indicate that it didn't have that address or that it couldn't understand that address.
Q. In the Microsoft accused products, and

specifically, the PeerNet interfaces, do those use regular domain names, or do they use something different?

A. They use something different. They use -- remember that long string of characters that were numbers and letters and dots followed by another string? That -- that name is not a conventional domain name either.

Q. What happens if that Windows PeerNet name -- peer name was sent to a regular DNS -- regular standard DNS server?

A. You would get an error returned, and I've tested and verified that myself.

Q. Just like a secure domain name that's listed in the '180 patent?

A. Yes, sir.

MR. McLEROY: Pass the witness.

THE COURT: Any recross?

MR. POWERS: Yes, Your Honor, very brief.

THE COURT: It's going to have to be. You're out of time.

MR. POWERS: Then I'll make it very brief.

RECROSS-EXAMINATION

BY MR. POWERS:

Q. Just two subjects, Dr. Jones.

One, you were asked just then by VirnetX's lawyer about the demonstration that Mr. Pall gave regarding ebay.com.
Do you recall that?
A. Yes, sir, I do.
Q. Now, the computers that were set up were not actually connected to the internet, were they?
A. They were not.
Q. So it's not going to find ebay.com, is it?
A. No, it's not.
Q. And ebay.com was not in the address book, was it?
A. No, sir, it wasn't in the address book.
Q. Secondly, with respect to Aventail -- could you get Exhibit 362, Plaintiff's Exhibit 362, in front of you, please?
Now, this is an SAIC document, correct?
A. Yes, sir, I believe it is.
Q. If you could turn to Page 27.
A. Is that marked 27 down at the bottom, or the page -- which --
Q. Marked 27 down at the bottom.
A. Okay, sir. I'm there.
Q. And if you go --
MR. POWERS: Chris, could you bring up --

just about, oh, 60 percent down, there's a discussion of VPN system providers. See if you can pull that out.

Well, let's get a little less text, if we could. Do you see where I'm referring to? About 60 percent down.

Q. (By Mr. Powers) And VPN starts on the far right-hand side, Dr. Jones.

A. Yes, sir, I do.

Q. And it says VPN system providers in the parenthetical, and the first one it lists is Aventail.

Do you see that?

A. Yes, sir.

Q. This is a situation where SAIC is calling Aventail a VPN system provider, right?

A. I believe it is. I haven't examined this document, sir.

MR. POWERS: No further questions, Your Honor, but we would offer PX362.

THE COURT: Okay. Any objection?

MR. McLEROY: No, Your Honor.

Two follow-up questions?

THE COURT: Yes, uh-huh.

That exhibit will be admitted, and you may redirect.

REDIRECT EXAMINATION

BY MR. POWERS:

Q. Professor Jones, do you still have Plaintiff's 362 in front of you?

A. Yes, sir.

Q. What is the date of that document?

A. I don't know, sir. July 8th, 1999, I believe is the -- is the date.

Q. Okay. At that time, had Judge Davis defined the term VPN yet?

A. No, sir, he had not.

Q. Is it at all possible that SAIC could have been applying the Court's definition of VPN when they were?

A. No, sir.

MR. McLEROY: Pass the witness.

THE COURT: Okay. Anything further?

MR. POWERS: No, Your Honor.

THE COURT: Okay. Very good.

All right. You may step down. Thank you.

All right. Microsoft have any further evidence -- I'm sorry. VirnetX?

MR. CAWLEY: VirnetX has no further evidence and rests, Your Honor.

THE COURT: All right. VirnetX rests.

Microsoft finally closes?

MR. POWERS: Yes, Your Honor.

THE COURT: And VirnetX finally closes?

MR. CAWLEY: Yes, Your Honor.

THE COURT: All right.

All right, Ladies of the Jury. That concludes the evidence stage of the case. I think it was a week ago today that we did the opening statements, and I told you we would, after that, go through the evidence. And then following the evidence, you will hear the Court's charge and then the final arguments of counsel.

But what I'm going to do now, I have some matters I have to take up with the attorneys, so I'm going to go ahead and let you recess for lunch, and we'll plan to start back here at 1:45. That will give you an hour and 20 minutes for lunch. We'll come back at 1:45, and at that time, you'll hear the charge and the arguments of counsel.

I, again, want to remind you of your instructions. Even though the evidence is all closed, you still should not discuss this case among yourselves or with anyone else.

So enjoy your lunch, and then we'll hear the arguments, and finally, later this afternoon, you'll be released to begin your deliberations.

I'm going to take about a five-minute

11:27 recess, and then I'll be back to visit with the attorneys.

11:27 So at this time, we are in recess until 11:27 1:45.

11:27 COURT SECURITY OFFICER: All rise.

(Jury out.)

(Recess.)

CERTIFICATION

I HEREBY CERTIFY that the foregoing is a true and correct transcript from the stenographic notes of the proceedings in the above-entitled matter to the best of my ability.

/s/__________________________ ______________________
SUSAN SIMMONS, CSR Date
Official Court Reporter
State of Texas No.: 267
Expiration Date: 12/31/10

/s/______________________ ____________________
JUDITH WERLINGER, CSR Date
Deputy Official Court Reporter
State of Texas No.: 731
Expiration Date: 12/31/10

EXHIBIT F12

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VIRNETX	*	Civil Docket No.
	*	6:07-CV-80.
VS.	*	Tyler, Texas
	*	
	*	March 15, 2010.
MICROSOFT CORPORATION	*	12:35 P.M.

TRANSCRIPT OF JURY TRIAL
BEFORE THE HONORABLE JUDGE LEONARD DAVIS
UNITED STATES DISTRICT JUDGE

APPEARANCES:

FOR THE PLAINTIFFS: MR. DOUGLAS CAWLEY
MR. BRADLEY CALDWELL
MR. JASON D. CASSADY
MR. LUKE MCLEROY
McKool-Smith
300 Crescent Court
Suite 1500
Dallas, TX 75201

MR. ROBERT M. PARKER
Parker, Bunt & Ainsworth
100 East Ferguson
Suite 1114
Tyler, TX 75702

APPEARANCES CONTINUED ON NEXT PAGE:

COURT REPORTERS: MS. SUSAN SIMMONS, CSR
Ms. Judith Werlinger, CSR
Official Court Reporters
100 East Houston, Suite 125
Marshall, TX 75670
903/935-3868.

(Proceedings recorded by mechanical stenography, transcript produced on CAT system.)

APPEARANCES CONTINUED:

FOR THE DEFENDANT:
MR. MATTHEW POWERS
MR. JARED BOBROW
MR. PAUL EHRLICH
MR. THOMAS KING
MR. ROBERT GERRITY
Weil Gotshal & Manges
201 Redwood Shores Parkway
5th Floor
Redwood City, CA 94065

MS. ELIZABETH WEISWASSER
MR. TIM DeMASI
Weil Gotshal & Manges
767 Fifth Avenue
New York, NY 10153

MR. DANIEL BOOTH
Weil Gotshal & Manges
700 Louisiana
Suite 1600
Houston, TX 77002

MR. RICHARD SAYLES
MR. MARK STRACHAN
Sayles Werbner
1201 Elm Street
4400 Renaissance Tower
Dallas, TX 75270

MR. ERIC FINDLAY
Findlay Craft
6760 Old Jacksonville Highway
Suite 101
Tyler, TX 75703

* * * * * *

P R O C E E D I N G S

(Jury out)

11:35 COURT SECURITY OFFICER: All rise.

11:35 THE COURT: Please be seated.

11:35 All right. Does Plaintiff have any motions it wishes to make?

MS. CASSADY: Your Honor, our star quarterback has appeared to disappear from the --

THE COURT: Okay. I'll take that as a no then, right?

MS. CASSADY: We do have some motions, Your Honor.

THE COURT: Oh, okay.

MR. CALDWELL: You mind if I go grab Mr. Cawley?

THE COURT: That will be fine.

In the meanwhile, does Defendant have a motion they wish to make?

MR. POWERS: Yes, we do, Your Honor.

Before we begin, though, I want to ask the Court if I may take my leave. If all you're going to handle is instructions, verdict form, and the JMOL motions, Mr. Bobrow is going to handle.

If there was something else, I was going to stay for that, but if that's what it is, I'd like the Court's permission to leave for now.

THE COURT: Permission granted.

MR. POWERS: Thank you, sir.

THE COURT: All right.

MR. CAWLEY: Sorry, Your Honor.

THE COURT: Yes.

MR. CAWLEY: I didn't know we were back in.

Are we ready to take up Plaintiff's JMOLs?

THE COURT: Plaintiff have a motion to make?

MR. CAWLEY: Your Honor, the Plaintiff, VirnetX, makes its motions for judgment as a matter of law at the close of the Defendant's case-in-chief.

And pursuant to the agreement of the parties and the permission of the Court, we have agreed that this may be done at this time as if it were done immediately following the close of the Defendant's case.

I'd like to make these motions in two sets.

The first is a set of three that I'd like to call to the particular attention of the Court, and then I've got a second set that I'm going to make that I'm sure the Court will be quite attentive to as well.

But these are the ones -- these first three are the ones that I'd really like to highlight for purposes of the discussion.

The first is, on best mode on the '135 patent, the Defendant has asserted the defense of invalidity based on the failure to disclose the inventor's best mode of practicing the invention.

We have heard no evidence whatsoever during the course of the trial about what the best mode would be or certainly about the Defendant's knowledge of that and their failure to disclose the best mode.

So we would submit that as a matter of law, that defense fails for lack of any proof whatsoever.

THE COURT: Okay. Response?

MR. BOBROW: I have no objection. As Your Honor knows, we asked that the jury instruction, in fact, on that be pulled, and as I understand it, it was.

THE COURT: Okay. So with defense counsel's agreement, that motion is granted.

MR. CAWLEY: All right. The second of this category is a similar argument of written description of the '135 patent.

Once again, that's a factual inquiry. There has been no evidence offered whatsoever as to what one of skill in the art would have perceived to be the adequacy of the written description supporting the certain claims.

THE COURT: Response?

MR. BOBROW: Same position, Your Honor. We don't oppose. It was --

THE COURT: All right. Motion is granted.

MR. CAWLEY: And the third of this category is Microsoft's counterclaim on the invalidity of Claim 7 of the '135 patent. As the Court may recall, the Plaintiff withdrew that claim and is not asserting it.

Microsoft, however, did not withdraw its counterclaim as to invalidity. However, there has been no proof offered during the course of the trial that Claim 7 of the '135 patent is invalid.

THE COURT: Okay.

MR. BOBROW: We would withdraw that without prejudice, Your Honor.

MR. CAWLEY: Well, I think --

THE COURT: I think it's a little late for --

MR. BOBROW: But it was not put into the case at the beginning. In other words, there was nothing in the Court's instructions or the parties' briefs that said that our counterclaim on Claim 7 was in.

The Plaintiff withdrew that claim. We did not put forward, either in the materials going in to the Court, that that was still an issue. So that was never litigated.

So, certainly, it should be withdrawn only without prejudice. Should this claim ever be asserted against us again, we would have the opportunity to litigate that claim. But as things stand now, that claim was not in the case. Only Claims 1, 10, and 12 of the '135 patent were in this case.

MR. CAWLEY: They have a live counterclaim on that claim, which they do, Your Honor. It's in the case. They have chosen not to offer any evidence on it, and that's appropriate for judgment as a matter of law.

THE COURT: When they withdrew their assertion as to Claim 7, did -- Microsoft, did you withdraw your counterclaim as to the invalidity?

MR. BOBROW: In a sense, we did, because it was not put forward in the materials pretrial that said, we're going to try this. They dropped Claim 7 on the eve of trial, and we simply -- the issue then was moot. We did not put forward and litigate Claim 7 at all.

And so certainly, any issues that as to Claim 7 are withdrawn then without prejudice for Microsoft to later challenge that claim.

THE COURT: I'm going to take that one under advisement.

MR. CAWLEY: All right. Now, Your

Honor --

THE COURT: There's nothing in the charge as to Claim 7, right?

MR. BOBROW: That's right.

MR. CAWLEY: I think that's correct, Your Honor.

MR. BOBROW: That's correct.

MR. CAWLEY: Now, the second category is some motions that I'm going to make now, and in the interest of time and efficiency, Your Honor, I will say that all of these are based on failures of proof.

And we are prepared to drill as deeply down into the evidence in the record as Your Honor would care to, but I -- but I -- you know, unless -- unless Your Honor -- I mean, I'm going to do what I need to do to make my motion and preserve my record, and if Your Honor feels as though I'm giving it short shrift and that we should get more deeply into the facts --

THE COURT: Give it short shrift, and if I want to jump in somewhere, I will.

MR. CAWLEY: All right. Thank you. The first, as of this category, anyway, is, we move for judgment as a matter of law as to direct infringement of the '135 patent. VirnetX seeks judgment under Rule 50 that it has established as a matter of law that

Microsoft directly infringes Claims 1, 10, and 12 of the '135 patent.

This motion is as to Windows XP, Windows Vista, Live Communications Server 2003, Live Communications Server 2005, Office Communications Server 2007, Office Communicator 2005, Office Communicator 2007, Messenger 5.0, Messenger 5.1, and Live Meeting Console.

VirnetX has established as a matter of law that the -- those accused products that I just named meet each claim under the Doctrine of Equivalents with testimony from Professor Jones that the website limitations are literally present or practiced by the '135 patent accused products.

Second, as to direct infringement of the '180 --

THE COURT: Just a moment. That motion is denied.

MR. CAWLEY: Yes, Your Honor.

As to direct infringement of the '180 patent, VirnetX seeks judgment under Rule 50 that it has established as a matter of law that Microsoft directly infringes Claims 1, 4, 15, 17, 20, 31, 33, and 35 of the '180 patent in Windows XP and Windows Vista.

Professor Jones has testified that the

limitations of the claims are satisfied in the accused products and that no reasonable jury could find otherwise.

THE COURT: All right. Motion is denied.

MR. CAWLEY: Next, VirnetX moves for judgment as a matter of law on inducement of the '135 patent and '180 patents. The evidence conclusively establishes that Microsoft took actions, such as marketing, participating in conferences, and leasing material that accuses others of infringing the patents.

There is evidence that the patents were directly infringed by Microsoft and others. There is undisputed evidence that Microsoft was aware of the patents and knew or should have known that the acts constituted and encouraged infringement.

And as I said, there is evidence of direct infringement, and there is evidence that Microsoft should have known that its encouragement or instruction would result in others infringing the claim. This evidence is so compelling that no reasonable jury could find otherwise.

THE COURT: Motion is denied.

MR. CAWLEY: Next, contributory infringement of the '135 patent.

Microsoft -- excuse me -- VirnetX has

established conclusively that Microsoft has sold, offered for sale, or imported a material component of the accused products or a material component used in the practicing method that is not a staple article of commerce suitable for substantial non-infringing use and that Microsoft had knowledge that the component was so made and adapted.

As already established, VirnetX has offered evidence that Microsoft knew of the '135 patent, and no reasonable jury could find otherwise.

THE COURT: Motion is denied.

MR. CAWLEY: VirnetX moves for judgment as a matter of law on its willfulness claims. It has proved by clear and convincing evidence that Microsoft willfully infringed the '135 and '180 patents; that it was aware of the patents; that it acted in spite of an objectively high likelihood that its actions infringed a valid patent, and no reasonable jury could find otherwise.

THE COURT: Motion is denied.

MR. CAWLEY: Microsoft -- VirnetX, that is, moves for judgment as a matter of law on damages. The evidence shows that it is entitled to a reasonable royalty in the amount of $158,700,000 for the '135 patent, and $83.6 million for the '180 patent, and no reasonable jury could find otherwise.

THE COURT: Motion is denied.

MR. CAWLEY: Likewise, VirnetX moves for judgment as a matter of law on the defenses of anticipation of the '135 and '180 patents on the grounds that all asserted references lack one or more central elements to establish invalidity, and no reasonable jury could find otherwise.

THE COURT: Motion is denied.

MR. CAWLEY: And VirnetX, finally, in this category, moves for a judgment as a matter of law on obviousness of the '135 and '180 patents on the ground that Microsoft has failed to meet its burden to produce clear and convincing evidence that any of the asserted claims of those patents would have been obvious at the time of filing to one of skill in the art, and no reasonable jury could find otherwise.

THE COURT: Motion is denied.

MR. CAWLEY: Thank you, Your Honor.

THE COURT: Thank you.

Defendant have any motions?

MR. BOBROW: Yes, Your Honor, we do.

Your Honor, we have a number of motions. Let me begin by stating that we did file a formal JMOL motion this morning, but, obviously, I'm prepared to put these on the record now for you and for your consideration.

THE COURT: If you'd like to just rest on your written motion...

MR. BOBROW: Well, we did submit the motion, but we do think that it is appropriate to go forward on this basis as well, setting forth for the record the motions that we are making.

THE COURT: All right.

MR. BOBROW: First of all, on the question of infringement, Microsoft moves for judgment as a matter of law on the question of infringement -- direct infringement of the '135 patent, that no reasonable jury could find that Microsoft directly infringes the asserted claims of the '135 patent.

There was overwhelming evidence that there is no anonymity; that there is no website; and that there is no gatekeeper computer.

And in addition, there is no evidence that Microsoft employees directly infringe or that making or licensing the software that's been accused to end users constitutes direct infringement.

THE COURT: Motion is denied.

MR. BOBROW: Secondly, Microsoft moves for judgment as a matter of law on the question of inducement of infringement of the '135 patent. No reasonable jury could find that Microsoft induced infringement of the '135 patent.

There is no evidence of knowledge before 2006 of the patent. There is no evidence of knowledge by Microsoft of infringement. There is no evidence of intent to cause the acts that Microsoft purportedly knew would infringe, and there is no evidence of intent to encourage infringement.

Of course, there also is no proof of direct infringement, and therefore, the motion should be granted.

THE COURT: Motion is denied.

MR. BOBROW: Your Honor, Microsoft next moves for judgment as a matter of law on the question of contributory infringement of the '135 patent. No reasonable jury could find contributory infringement by Microsoft of the '135 patent.

To begin, the software at issue cannot, as a matter of fact law, be a component. The component that the Plaintiff has focused on is the wrong thing. It is not what Microsoft sells, but instead is a specific string of code. There is no basis to find that that is a component as a matter of law.

In addition, there is no evidence of the requisite knowledge that the feature at issue infringes or that Microsoft knew that the purported component was adapted for infringement.

And in addition, the evidence shows that Microsoft knew of substantial non-infringing uses. And so there has not been any showing that the accused products were especially made or especially adapted for infringement.

Finally, there is no evidence of a lack of substantial non-infringing uses.

THE COURT: Motion is denied.

MR. BOBROW: Next, Your Honor, on the '180 patent, Microsoft moves for judgment as a matter of law of no infringement on direct infringement, induced infringement, and contributory infringement -- I'm sorry -- direct infringement and induced infringement. There is no claim -- that claim has been withdrawn on contributory negligence by VirnetX.

First of all, on direct infringement, no reasonable jury could find that Microsoft directly infringes the asserted claims of the '180 patent. There has been overwhelming evidence that the accused software does not include and does not use a virtual private network and does not use and there is not included a secure computer network address.

Furthermore, there is no evidence that any Microsoft employees use the accused software, and in addition, the evidence showed that the software would not be invoked -- the accused software would not be invoked in normal operation, and finally, that making or licensing the software to end users does not constitute direct infringement.

THE COURT: Okay. Motion is denied.

MR. BOBROW: Microsoft next moves for judgment as a matter of law on the question of inducement of the '180 patent. No reasonable jury could find that Microsoft induces infringement of the '180 patent.

We introduced substantial evidence of non-infringing uses. We demonstrated certainly that since this claim was only filed in after this lawsuit was filed, we showed substantial defenses to the arguments and compelling arguments on the question of invalidity, so as a result, certainly, there's been no showing that Microsoft intended to cause acts of infringement, knew of the acts of infringement, or intended in any way to encourage infringement.

THE COURT: Motion is denied.

MR. BOBROW: Furthermore, Your Honor, Microsoft moves for judgment as a matter of law that liability for indirect infringement must be limited under the Dyna Corp case to acts of direct infringement.

Any liability for indirect infringement of either patent must be limited by the quantifiable acts of direct infringement, and we move on that ground.

THE COURT: Motion is denied.

MR. BOBROW: Microsoft next moves for judgment as a matter of law on the question of invalidity.

And specifically, first of all, on the question of anticipation, Microsoft moves for judgment as a matter of law that no reasonable jury could fail to find, by clear and convincing evidence, that the asserted claims of the '135 and '180 patents are anticipated.

We submitted evidence -- overwhelming evidence on three pieces of prior art, none of which was in front of the Patent Office.

Microsoft's NT 4 software with the PPTP, VPN, and AutoDial; second, Dynamic VPN; and third, the Aventail software guide, all of those prior art, none before the Patent Office, and all of that, as a matter of law, provides clear and convincing evidence of anticipation of all of the claims.

THE COURT: Motion is denied.

MR. BOBROW: Microsoft next moves for judgment as a matter of law on the question of obviousness. No reasonable jury could fail to find, by clear and convincing evidence, that the asserted claims are obvious in light of the prior art just mentioned, the Microsoft NT 4 with PPTP, VPN, and AutoDial, Aventail 3.1, and the DVPN demonstration.

The obviousness certainly should be found as a matter of law, both based upon those references by themselves, that is, single reference of obviousness, or when the various materials for each reference are combined together, those prior art references render the claims invalid as a matter of law.

THE COURT: Motion is denied.

MR. BOBROW: Microsoft next moves for a judgment as a matter of law on the question of willfulness. No reasonable jury could find, by clear and convincing evidence, that Microsoft willfully infringed either the '135 or '180 patents because neither prong of the Seagate case has been satisfied.

Certainly, the objective prong has not been met. We have put forth compelling evidence of non-infringement and validity, and certainly, the cases have certainly shown that it is beyond a close case, and indeed, one on which we're entitled to judgment as a matter of law.

On the subjective prong, certainly, there's been no evidence that Microsoft believed that there was an objectively high likelihood that the accused software would infringe any of the patents.

THE COURT: Motion is denied.

MR. BOBROW: Microsoft then moves for judgment as a matter of law on the question of damages. There is insufficient evidence, as a matter of law, to support Plaintiff's requested damages, or for that matter, any damage award over $15 million.

To begin, the testimony of Mr. Reed should have been excluded for all of the reasons set forth in Microsoft's Daubert motion pretrial.

Secondly, the evidence on the rate base is insufficient to support the requested damages award or, again, any award over $15 million, based upon the improper reliance on the entire market value, based upon the failure to apportion, and based upon the inclusion of foreign acts of infringement or alleged infringement.

In addition, the evidence of the royalty rate was insufficient to support the alleged claim or, again, any claim over $15 million. Again, there was no apportionment. The bases for the rate were essentially noncomparable licenses, and the benchmark licenses that were cited bore no royalties at all.

In addition, the requested amount of something on the order of $242 million is not a reasonable royalty, and in this context, is excessive and shocks the conscience and is manifestly an excessive amount, and we move on that ground as well.

THE COURT: Motion is denied.

MR. BOBROW: And if I may, Your Honor, one final point on our judgment as a matter of law on contributory infringement. I should have mentioned as well an additional ground for that motion. And I apologize.

But the item that had been identified as the -- essentially, the automatic connection feature, in addition to not being a component, it is also not a material or apparatus for use in a patented method, and we move on that basis as well.

THE COURT: Over -- denied.

Anything further?

MR. BOBROW: That's all, Your Honor.

THE COURT: All right. Plaintiff have any objections to the Court's charge?

MR. CALDWELL: Yes, Your Honor.

First, just to get this out of the way, if it's okay and we have the Court's permission, the parties have agreed that by submitting jury instructions with respect to the Court's claim constructions, the parties are not waiving and hereby expressly preserve their contentions in the Markman briefing and the arguments to the Court and reserves the right to appeal on these claim construction grounds.

THE COURT: Is that so agreed?

MR. BOBROW: Yes, it is, Your Honor, and neither side is waiving and is specifically preserving on the claim construction.

THE COURT: So noted.

MR. CALDWELL: And I have an observation about the verdict form. Are we going to get that -- get to that in a minute?

THE COURT: Sure.

MR. CALDWELL: Okay.

MR. BOBROW: Or you can cover whichever one you would like to.

MR. CALDWELL: Well, I just -- whichever one Your Honor has handy. We'll start with the charge.

THE COURT: I've them both handy.

MR. CALDWELL: Okay. In the charge, at Page 9 --

THE COURT: Okay.

MR. CALDWELL: -- I direct Your Honor to

the second full paragraph that begins: A patent claim is directly infringed only if the accused product or method includes each and every element of the patent claim.

Following that sentence, VirnetX has proposed and we object to the absence of an instruction that the accused product infringes a claim but is reasonably capable of satisfying the claim element, even though it may also be capable of non-infringing modes of operation, citing the Hilgraeve Corporations case.

Your Honor gave that instruction in Mass Engineering, and it was actually not in the i4i instructions, but I think that was because i4i only involved a method claim, and so the issue of the apparatus being capable of was just sort of a non-issue for i4i, and that's why it was absent and -- absent there.

THE COURT: All right. Give me the sentence again very slowly.

MR. CALDWELL: An accused product infringes the claim --

THE COURT: Slower than that.

MR. CALDWELL: Okay. I'm sorry.

An accused product infringes a claim if it is reasonably capable of satisfying the claim element even though it may also be capable of non-infringing modes of operation.

THE COURT: Response?

MR. BOBROW: Yes, Your Honor.

On that request, which I believe was not given in the i4i case, the issue there is that -- is that instruction can be very confusing in this context and I think prejudicial to the issue of what the jury needs to do.

The jury needs to look at the claim limitations and determine whether they are met in the methods, whether they're met in the products, whether they're met in the systems, and whether they're met in the computer-readable storage media claims.

And what, I think, this has the risk of doing is essentially lowering the Plaintiff's burden of proof by suggesting to the jury that somehow they can apply something that is not the limitations of the claim, but rather something much more vague and much more amorphous than that.

I'm afraid it would lower, essentially, VirnetX's burden of proof where it must prove that all of those limitations are there either literally or under the Doctrine of Equivalents.

THE COURT: All right. I'm going to give

this instruction, the same one that Microsoft -- I mean, that VirnetX suggested, except I'm going to strike the reasonably -- it-is-reasonably-capable-of language and change satisfy to satisfies.

So it will read: An accused product infringes the claim if it satisfies the claim elements even though it may also be capable of non-infringing modes of operation.

MR. CALDWELL: Just for the record, VirnetX objects to the exclusion of capable of, given that that is the law from the Federal Circuit, in terms of an apparatus. It doesn't have to necessarily always infringe as long as the apparatus is capable of, so...

THE COURT: What's your opinion on that?

MR. BOBROW: Well, I think the problem, in part, with that claim, as you've revised that language, Your Honor, is that it may be confusing for the jury on the question of indirect infringement because we have issues of substantial non-infringing uses and all of that, and I'm afraid, again, the jury may be confused in terms of understanding what it means when something might have other uses.

THE COURT: Well --

MR. BOBROW: That issue can be highly relevant in those contexts, so we would still object.

THE COURT: All right. I think the instruction is proper under the facts of this case, and I will give it the way that Microsoft -- I mean, that VirnetX originally proposed with the --

So it will read: An accused product infringes a claim if it is reasonably capable of satisfying the claim elements, even though it may also be capable of non-infringing modes of operation.

MR. CALDWELL: Yes, Your Honor.

THE COURT: Okay. What's next?

MR. CALDWELL: Ready for -- ready for the next one?

THE COURT: Uh-huh.

MR. CALDWELL: It's on Page 12.

THE COURT: Okay.

MR. CALDWELL: And do you see the numbered elements down toward the bottom.

THE COURT: Uh-huh.

MR. CALDWELL: And this is, I guess, as much a request for clarification as it is an objection, I would say.

In No. 2, after the words patented method, VirnetX had requested just a clause there, comma, which can be software, comma, because we believe that the law supports the argument in Microsoft's motions for JMOL.

I believe the law supports that the component in a contributory infringement analysis absolutely can be software, and we were hoping to make that express. So I don't know that that's the same thing as saying the sentence Your Honor has is legally error, but...

THE COURT: Any response?

MR. BOBROW: Well, Your Honor, our position -- we object to that. Our position is, is that software cannot be a component under the AT&T/Microsoft case. So we would object to that -- the inclusion of that language.

MR. CALDWELL: Your Honor, we have also the i4i Federal Circuit opinion, which I meant to cite to you and which also cites the RICO case.

THE COURT: Because there seems to be a dispute about it, I will insert the language which can be software, patent which can be software.

MR. CALDWELL: Thank you.

THE COURT: All right. What else?

MR. CALDWELL: Let me breeze through this.

The next observation is on Page 24, Your Honor.

THE COURT: Okay.

MR. CALDWELL: There is -- the first full

12:04 paragraph that begins with to be relevant.
12:04 THE COURT: Okay.
12:04 MR. CALDWELL: And that first sentence,
12:04 we -- or that whole paragraph was from Microsoft's
12:04 proposals, not VirnetX's.
12:04 At this point, VirnetX is not objecting to
12:05 the first sentence, but VirnetX objects to the second
12:05 sentence beginning with, if a secondary consideration,
12:05 on the grounds that at best, it's repetitious or
12:05 redundant of the first sentence to the extent the first
12:05 sentence properly captures the law, but beyond that, it
12:05 appears to be expanding the scope of what the law is.
12:05 In other words, VirnetX is not objecting
12:05 that the jury should consider a nexus between the
12:05 secondary consideration.
12:05 THE COURT: So you're objecting -- you're
12:05 asking that that last sentence of the paragraph be
12:05 stricken?
12:05 MR. CALDWELL: Yes, Your Honor, because we
12:05 think the first sentence is proper.
12:05 THE COURT: Response?
12:05 MR. BOBROW: I think the last sentence,
12:05 Your Honor, helps a lay jury understand what that word
12:05 in quotes nexus means. I think this sentence certainly
12:05 gives that first sentence much more meaning and will

help the jurors understand what the requirements are for the secondary or objective considerations to be relevant.

THE COURT: Objection is overruled.

What's next?

MR. CALDWELL: The next one I would have is with the verdict form, Your Honor.

THE COURT: All right.

MR. CALDWELL: And this is just simply a matter of clarification. I -- my copy has actually been stolen and taken to the back room.

But the first three questions on the verdict form refer to Column 1, Column 2, Column 3, and VirnetX is merely suggesting that we entitle -- instead of Issue 1, Issue 2, and Issue 3 on the second page, that we entitle the headings of the top of the second page Your Honor is looking at -- we entitle those Column 1, Column 2, Column 3.

THE COURT: Instead of Issue 1, Issue 2?

MR. CALDWELL: Yes, Your Honor, just for clarification.

THE COURT: All right. We'll replace column -- issue with column, if there's no objection.

MR. BOBROW: Your Honor, we do have other objections to the form, but not with that one per se.

THE COURT: All right. We'll change issue to column in those three spots on the second page.

All right. Anything further?

MR. CALDWELL: No, Your Honor.

THE COURT: All right. Microsoft have any objections?

MR. BOBROW: Your Honor, we do have a number of objections, and we would like the Court to know we have a spent a substantial amount of time going through these, and I'll be as diligent and expeditious as we can.

Would the Court prefer to start with the verdict form, since you were just there?

THE COURT: All right.

MR. BOBROW: So, first of all, on the verdict form, Microsoft objects to the infringement questions here, question No. 1 in the way it's been divided up. In particular, we object that there has been no division for direct, induced or contributory infringement. Those, of course, have separate elements and we think they should be broken out separately.

In addition, the infringement question does not break out the questions for infringement by the different accused software for -- for the different accused patents.

THE COURT: Okay. That's all covered in the instructions. It's overruled.

MR. BOBROW: Secondly, on the question of validity, we object on the grounds that, again, anticipation and obviousness have not been broken out, creating some -- what we consider to be some general verdict issues. We have -- it does not break the issues out by prior art reference.

We also object that it includes the clear and convincing burden of proof when all the art that we have relied upon was indisputably not before the Patent Office.

We also object to the submission of the obviousness question to the jury and also the non-submission to the jury of the underlying fact questions for obviousness. We also object on that ground.

THE COURT: Okay. Your objection's overruled.

MR. BOBROW: On damages, again, we object to the failure to break up the damages to ask about lump sum versus running royalty, and we think that there's been evidence in the case to that effect and that the jury should look at that question.

In addition, there has been evidence

presented to the jury on future damages and the form as it is now will leave that issue vague, and when it comes to any remedies for injunction, will make that issue difficult, if not impossible, to resolve. So we object to the form in which the amounts has been set forth for money damages.

THE COURT: Objection Is overruled.

MR. BOBROW: In addition, we object to the form for the failure to ask the jury to specify the term covered by the royalty, whether it's up through trial or going forward, and we also object to the omission from the form of a line that would ask the jurors to determine the number of directly infringing sales or installations, as it were, under the Dyna Corp. Case.

THE COURT: Overruled.

MR. BOBROW: Your Honor, I'd like to now move to the Court's charge.

THE COURT: All right.

MR. BOBROW: And one point in addition to the point made earlier about that both parties are preserving on the question of claim construction. Related to that, of course, is that we had requested that Appendix B be modified by motion to include the requirement of anonymity that the Court has said is there but is not in Appendix B, and we object to the --

the non-inclusion of the word anonymity in Appendix B per our prior motion that the Court denied.

THE COURT: Okay. Overruled.

MR. BOBROW: Turning to the Summary of Contentions. This is on page 4.

THE COURT: Let me just clarify. Your last request, I don't think there's anything, and correct me if I'm wrong, but there's any disagreement between the parties that anonymity is required. The only dispute that's been raised in the evidence is to -- to what constitutes anonymity.

Is that not correct?

MR. BOBROW: Your Honor, that is correct. Our request was to include that requirement in Appendix B so that the jurors would have that in front of them in the course of their deliberations.

THE COURT: Okay. Overruled.

MR. BOBROW: So in the Summary of Contentions which is paragraph 2, we have several concerns about the way that the summary of the infringement allegations as made.

To begin, in the first part, about four or five lines down, it talks about making, using, selling, offering to sell and importing into the United States the patented apparatuses and/or using the patented methods in Microsoft's accused software products.

I don't think that Microsoft objects that that does not accurately describe the state of play, but it doesn't describe the Plaintiff's allegations here. And we would propose the following as an alternative: That alternative would be to say by making, using, selling, offering to sell, or importing into the United States patented systems or apparatuses or by using Microsoft's accused software to perform the patented methods.

THE COURT: Plaintiff's response? Why don't you read that again very slowly just so...

MR. BOBROW: Certainly, Your Honor.

By making, using, selling, offering to sale or -- as opposed to and -- or importing into the United States patented systems or apparatuses, or by using Microsoft's accused software to perform the patented method or methods.

MR. CALDWELL: I don't think we have any problem with that, Your Honor.

THE COURT: All right. Let me ask, Ms. Li, did you get that down?

Yeah. Read it one more time very slowly, please, because we're making these changes real-time, real-time as you speak.

MR. BOBROW: Yes. Thank you.
By making, using, selling, offering to sell, or importing into the United States.
THE COURT: Okay. And so you delete the word and and replace it with or, right?
MR. BOBROW: Yep. Yes, that's correct.
THE COURT: Importing -- let me read it. Importing into the United States, strike the word the. Or no. Let's see. No. The stays in, doesn't it?
MR. BOBROW: No. We would ask that that be taken out.
THE COURT: All right. Strike the. And then patented systems.
MR. BOBROW: Or apparatuses. Or by using Microsoft's accused software to perform the patented methods.
THE COURT: Okay. Let me read it one more time to be sure we've got it right.
By making, using, selling, offering to sale or importing into the United States patented systems or apparatuses or by using the patented -- or by using Microsoft's accused software to perform the patented methods.
MR. BOBROW: Yes.
THE COURT: Okay. That's sustained.

What's next?

MR. BOBROW: The next is to -- a little further down on page 4, this dealing with the '135 patent where it says who -- the second line from the bottom, who make or use the patented apparatuses or perform the patented methods with Microsoft's accused software products.

We propose to replace that so that it more accurately lines up with the allegations in the -- in the language of the claims. Who make or use the patented systems or perform the patented methods.

THE COURT: So you would be replacing apparatuses with systems.

MR. BOBROW: And also deleting the last part, with Microsoft's accused software products.

THE COURT: So you'd strike the last clause, with Microsoft's accused software products.

MR. BOBROW: That's what we propose, Your Honor.

THE COURT: Any objections to that change?

MR. CALDWELL: Still digesting it. Just one second.

THE COURT: Okay.

MR. CALDWELL: I don't think we have an objection. One second.

No objection, Your Honor.

THE COURT: All right. Granted.

MR. BOBROW: On page 5, Your Honor, this is dealing with the '180 patent. Second and third lines there's a clause that says, who make or use the patented apparatuses or perform the patented methods with Microsoft's accused software products?

THE COURT: Same change?

MR. BOBROW: I apologize.

THE COURT: Replace apparatuses with systems?

MR. BOBROW: We would propose, Your Honor, to strike that in its entirety because I think that it doesn't capture what is being asserted here in the case. The assertion is is that we are inducing others, but this is suggesting others who make these various items. It seems that the better course would just be to say that Microsoft is inducing indirect infringement of the '180 patent by others, or, at the very least, to delete the phrase, with Microsoft's accused software products.

THE COURT: Response?

MR. CALDWELL: We disagree with that, Your Honor. And actually -- and just to answer Your Honor's question a little more directly, it can't be the same change we made for the '135 patent because the '180 patent, whereas the '135 patent has method and system, this one also has computer-readable media claims.

THE COURT: Okay.

MR. CALDWELL: And when folks install that on their computer, they make the apparatus computer-readable media, et cetera.

THE COURT: Okay. That objection's overruled.

MR. BOBROW: Your Honor, at the bottom of page 3, in the burden of proof, we object to the sentence that, Microsoft has the burden by clear and convincing evidence.

THE COURT: That's overruled.

MR. BOBROW: Turning to instruction 6 on page 8, Microsoft had asked for an instruction on the different types of claims that the jury is considering because they have different requirements: Computer-readable media, system, apparatus, method. We noted the Court did not include that proposed language.

THE COURT: Objection's overruled.

MR. BOBROW: On page 9, Your Honor, in the third full paragraph that begins, a person can directly infringe a patent without knowing that what it is doing is an infringement, all the way down to the end of that paragraph, which is two sentences, we object to both of those sentences, again, on the grounds that it is an incorrect statement of the law, particularly for inducing infringement or contribution or contributory infringement, because in that context, knowledge and intent are requirements and here it, I think, will improperly suggest to the jury that you can directly infringe by inducement or by contribution even if you don't know what you're doing. And that's not what the law is.

THE COURT: Response?

MR. CALDWELL: Well, Your Honor, first of all, this is in the heading of Direct Infringement, and actually the paragraph says a person can directly infringe, and on the next sentence it says someone may also directly infringe. So the observation about that something might be different for contrib or induced is -- is, I think, in opposite. Besides, this is actually a correct statement of the law, and it came from the Court's instructions in i4i.

THE COURT: Okay. That objection's overruled.

MR. BOBROW: Your Honor, on page 10, Literal Infringement, we had requested an instruction essentially on the all limitations requirement for literal infringement, that, in effect, the literal infringement instruction provide that all limitations have to be met literally. Presently, the instruction does not say that but just talks about what one must provide for an individual limitation as opposed to all the limitations together.

THE COURT: Objection's overruled.

MR. BOBROW: Your Honor, on 6.2, page 11, VirnetX has proposed language which the Court adopted on the standard for active inducement.

We object to this instruction on a number of grounds.

To begin, we object that the instruction in paragraph 3 provides for the should have known standard, which we think is inconsistent with the law.

In paragraph 4, which provides the person has an intent to cause the encouraged acts we believe doesn't correctly state the law on the question of intent. That you must have more intent than that, and you must have intent to infringe.

We also object, further down the page in the paragraph that talks about advice of counsel which we think is inconsistent with the law, to bring that issue up in the context of induced infringement.

And then similarly, on page 12, similar to the objections already made, there are references to intent to cause the acts and also the should have known standard which we do -- which we do not think are correct statements of the law.

We had also asked for an instruction that the jury must determine the number of acts of direct infringement which was not included here.

THE COURT: All right. Objection's overruled.

MR. BOBROW: Your Honor, on contributory infringement, 6.3 on page 12 running over to 13, we have several objections.

First, in subparagraph 2 where it talks about a material component of the product or a material component used in practicing the patented method, this raises a similar issue as to what we have talked about before with respect to component, and we object on that ground. But it also misstates the statutory requirement here, because for the method, the operative language is a material or apparatus for use in practicing a patented process as opposed to a component. So we would object on that ground as well.

THE COURT: Objection's overruled.

MR. BOBROW: As mentioned before, we object to the use of the component here and that instruction is violating the -- and inconsistent with the AT&T Microsoft case.

We also object that the instruction does not tell the jury that they must find that -- that the component or material or apparatus was a material part of the invention that is essential to the advance over the prior art.

THE COURT: Objection's overruled.

MR. BOBROW: And further, we object that, again, the instruction asks the jury to focus on whether the component itself, not the product in which the component is bedded is or is not suitable for substantial non-infringing use. We think that that is not a correct statement of the law.

THE COURT: Objection's overruled.

MR. BOBROW: On the willfulness -- willfulness infringement instruction, 6.4, we have several objections. To begin, we had requested an instruction that gave some guidance to the jury on what the objective standard is. That instruction was not provided for. We are concerned that there is not enough guidance in the instruction for the jury to understand what that objectively high likelihood standard means or how to apply that instruction in practice. And we would object on that ground.

We had requested that language be

included, for example, about credible defenses to infringement and validity. And that language was not included by the Court.

THE COURT: Objection's overruled.

MR. BOBROW: On page 14, we object to the two subparagraphs concerning reasonable basis and good faith efforts. We think that these instructions impermissibly shift the burden to Microsoft to demonstrate either reasonable basis or good faith when, in fact, it is the Plaintiff's burden here by clear and convincing evidence to show that.

THE COURT: Objection's overruled.

MR. BOBROW: Your Honor, we further had requested language and an instruction providing guidance to the jury on what a reasonable basis for concluding that a claim was not valid or was not infringed, what that language meant. The Court declined to include that language in the instruction and we would object on that ground.

THE COURT: Overruled.

MR. BOBROW: We also requested in this section a sentence asking that you tell the jurors that simply notice that someone owns a patent doesn't give rise to a duty to investigate, and we asked that that be included in this instruction and it's not.

THE COURT: Overruled.

MR. BOBROW: Thank you.

With respect to invalidity, there were, again, any number of references to either No. 1, the clear and convincing burden and the presumption of validity. I see that, for example, at page 14, under section 7, we object in light of the proof that Microsoft admitted none of which was before the Patent Office.

THE COURT: Overruled.

MR. BOBROW: On page 15, there are a number of passages in this paragraph that discuss inherency and what that means. The -- at the beginning of the paragraph, the paragraph provides that for anticipation all the requirements must be present in a single previous device or described in a single previous device -- publication or patent. We had asked that inherency be included in there so the jurors knew that inherency was a way for something to anticipate and the Court declined to include that.

THE COURT: Overruled.

MR. BOBROW: In addition, Your Honor, we had objected to the phrasing of what inherency means. The Court is telling the jury that it means that something is always present in the prior art or always results from the practice.

Further down, it says that the elements are always present in the prior art or always a result. We believe the proper phrasing for that should be something that essentially is the natural result of the prior art or the use of the prior art.

THE COURT: Overruled.

MR. BOBROW: Your Honor, on obviousness, to reiterate, we had requested here that the Court make the legal determination of obviousness. That does not appear to be set forth in the -- in the Court's instruction.

THE COURT: Overruled.

MR. BOBROW: Once again, the clear and convincing burden appears here, and I understand Your Honor's ruling already on that, but we object to the clear and convincing burden.

THE COURT: Overruled.

MR. BOBROW: In the next paragraph on page 19, the Court has an instruction here that the jury should not consider what it learned from or about the patent during trial. One concern we have about this and objection to it, Your Honor, is that there are materials in the patent that actually are prior art. There are statements about what the prior art included and how the prior art worked and what the prior art was, and it seems to us that that sentence could be clarified.

THE COURT: Which instruction is that?

MR. BOBROW: This is 7.3, third paragraph down. This is an instruction on hindsight, and the part of it which Microsoft objects to is on lines 3 running over to 4 which said, essentially, that the jury can't consider what it learned about the patent during the trial.

THE COURT: Do you have a suggested change to that?

MR. BOBROW: Your Honor, the -- the suggested change that -- that we would propose would be to make clear that -- essentially what it learned about the claimed invention. Because again, it's proper for the jury to consider the prior art.

THE COURT: A response?

MR. McLEROY: No objection, Your Honor.

THE COURT: Okay. Where will this sentence be inserted?

MR. CALDWELL: I think, actually, it's just a substitution of instead of saying what you learned from or about the patent during the trial, it would be changed to what you learned from or about the claimed invention.

THE COURT: Agreed?

MR. BOBROW: Agreed.

THE COURT: All right. We'll substitute claimed invention for the word patent.

MR. BOBROW: On page 19, Your Honor, just below that there's an instruction on the question of motivation. We consider that instruction to be inconsistent with KSR and potentially suggesting to the jury that that's something that they must consider, and we object on that ground.

THE COURT: It's overruled.

MR. BOBROW: On page 20 in 7.3.1 in the description of the -- of the person of ordinary skill, Microsoft had proposed some language from the KSR case to make clear to the jurors that those of ordinary skill would employ inferences and create steps appropriate to his or her discipline that, essentially, making clear what a person of ordinary skill in the art does when looking at a matter. That requested instruction was not included, and we would object on that ground.

THE COURT: Overruled.

MR. BOBROW: On page 21, in the second full paragraph, there are references here to the field of endeavor. And in the field of endeavor, the Court has defined it in terms of the problems or issues that the inventor faced, and we believe that that is not the standard. The standard is broader than that.

And of course that the issues the inventor faced may be relevant, but it could be the standard we think should be reasonably related to any need or problem known in the field of endeavor including the problems or issues faced by the inventors.

THE COURT: Okay. Where is that on page 21?

MR. BOBROW: Yes, it is, Your Honor. It's in the second full paragraph.

THE COURT: All right. And tell me what change you're proposing and where it goes.

MR. BOBROW: Well, the change, Your Honor, would be at lines 3 and 5. It says, The reference must be reasonably related to the particular problem or issue the inventor faced or addressed. And we think that instead of that, the language should be as we requested in our proposed instruction that the reference must be reasonably related to any need or problem known in the field of endeavor, comma, including --

THE COURT: Just a second. Slow down a second.

MR. BOBROW: Certainly.

THE COURT: Any need or problem known in

12:32 the --

12:32 MR. BOBROW: The field of endeavor.

12:33 THE COURT: Okay.

12:33 MR. BOBROW: Comma, including the particular problem or issue the inventor faced.

12:33 And then the next --

12:33 THE COURT: All right. Just a moment. Before you go on, let me see if there's any objection to inserting that. I mean, if there's -- what Plaintiff's position is with regard to that proposed change.

12:33 MR. CALDWELL: Plaintiff's position is that the instruction Plaintiff proposed is actually the correct one. It's the one that was given in i4i against Microsoft, Your Honor.

12:33 Now that said, I mean, if -- if the issue of -- sorry.

12:33 THE COURT: Yeah. Objection's overruled.

12:33 What's next?

12:33 MR. BOBROW: Your Honor, next 7.3.3, differences over the prior art. We object to the second and third sentences of the first paragraph. In that section, we think that the instruction is an incorrect statement of the law. This section asks the jurors to focus on the differences between the prior art and the claimed invention, and then immediately says that they should not focus on those differences between the prior art and the invention.

We think that those sentences should be struck since, again, this is part of the obviousness analysis where the differences are the correct focus for the jury.

THE COURT: All right. Objections's overruled.

Anything further?

MR. BOBROW: Yes, Your Honor. I apologize. I'm just going through my notes.

Yes, we also object to several requested instructions that were not included. Microsoft had requested an instruction regarding the fact that motivation -- motivation combined is a factor but is not a requirement. We would ask that that instruction be included.

THE COURT: Overruled.

MR. BOBROW: We had also asked for an instruction that when there is a design need or market pressure to solve a problem and there are a finite number of identified predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. That also was not included.

THE COURT: Overruled.

MR. BOBROW: 7.3.4, Your Honor, additional considerations. These are the secondary considerations of non-obviousness.

We have two issues here. Issue No. 1 is that factor No. 4 is a factor that discusses copying of the invention.

The Court might remember that there was a stipulation before trial on that question of copying in terms of the parties not introducing evidence that either Microsoft did copy or Microsoft didn't copy and the like. And we think that there has been no evidence introduced on copying as a result and so this is not an appropriate factor to be listed in the jury instruction.

THE COURT: Response?

MR. CALDWELL: We're fine taking out No. 4 and just...

THE COURT: All right. No. 4 will come out and we'll re-number those 5 through 10.

MR. BOBROW: Your Honor, we also object to factor No. 7 on the question of whether or not others have taken licenses to use the invention. This was not a factor that either party's expert discussed in their testimony. It was not anything that was tied to the question of obviousness. And since there is no proof on that subject, we would propose striking No. 7 as well.

THE COURT: Any objection?

MR. CALDWELL: Yes, Your Honor. There is objection because their evidence of license is taken to the technology from VirnetX.

THE COURT: All right. And overrule the objection.

MR. BOBROW: Your Honor, another issue here. We had asked for an instruction on page 24, right after the numbered factors. We asked for a sentence and instruction that apprised the jury that the question of the relevance and relative importance of these various factors was for them to consider. The Court did not provide that instruction and we request that it be so given to the jury.

THE COURT: All right. Overruled.

MR. BOBROW: On to the question of damages. In Section 8.1, we had objected to the requirement as set forth in the instruction that the hypothetical negotiation is the required analysis. We think that the correct law is that it is one factor in the Georgia-Pacific analysis, and the language that essentially says that it is the -- the only perspective through which to analyze this is not a correct statement of the law.

THE COURT: Overruled.

MR. BOBROW: Microsoft also objects to the exclusion of an instruction we requested on a lump-sum royalty essentially saying that royalties can be running or lump sum, and there certainly has been evidence on a lump-sum royalty and we think that the jury should be instructed on it.

THE COURT: Overruled.

MR. BOBROW: We also object to the exclusion of an instruction that asks the jury and tells the jury that, essentially, that the number of acts of infringement limit the number of damages. This is from the Dyna Corp. Case. We think that that should be reflected in the instruction.

THE COURT: Overruled.

MR. BOBROW: We have concerns about the -- and object to the statement that the infringer's actual profits may or may not bear on the reasonableness of an award based on a reasonable royalty. We have -- we object that that violates the entire market value rule by having, essentially, profits on a system as a whole, on an operating system as a whole or a software as a whole as opposed to reflecting any sort of value of that which is accused of infringing. In this case which is a much, much, much smaller piece of the software at issue.

THE COURT: Overruled.

MR. BOBROW: Microsoft also objects to the sentence that says that the jury's determination does not depend on the actual willingness of the parties to the lawsuit to engage in such negotiations. The objection there, Your Honor, is that the jury will be asked to consider evidence of what actually happened in real life in the hypothetical negotiation, and the concern is that they will not understand that they may take into account actual license practices, actual licenses; for example, the SafeNet license that was rejected and the like.

THE COURT: Overruled.

MR. BOBROW: On the reasonable royalty factors, 8.2, paragraph 1, we object to the phrasing, whether the licensor has established a royalty for the patented invention such as by granting other licenses for a royalty. We had proposed different language than that.

Our concern with this is that this language could be misconstrued by the jury as suggesting that an established royalty could be met by, for example, one or two licenses which we think is not the law. It also does not provide that the jury should consider the royalties received by the licensor and it's the royalties received tending to prove or not prove the establishment of an established royalty.

THE COURT: Overruled.

MR. BOBROW: Your Honor, we had requested an instruction that we had labeled 8.3. This was an instruction on apportionment and the entire market value. The Court has declined to include that in its charge and we object to that exclusion.

THE COURT: Overruled.

MR. BOBROW: Your Honor, those are Microsoft's objections to the charge.

THE COURT: Very well. Thank you.

MR. BOBROW: Thank you.

We will be in recess until 1:00 o'clock. Please inform the jury they'll have an extra 15 minutes.

COURT SECURITY OFFICER: All rise.

(Recess.)

COURT SECURITY OFFICER: All rise for the jury.

(Jury in.)

THE COURT: Please be seated.

All right. Ladies of the Jury, I hope you had a good lunch. We all worked during most of the noon hour, so I think everyone had sort of an abbreviated lunch that's involved in the case, but I am going to give you your final jury instructions at this time.

I'm going to have my staff pass out to you a copy of the Court's charge, and you can follow along, if you wish, or -- but I would encourage you to not get too caught up in reading it that you don't listen. But we may get to some parts that I'll just refer you to and let you read at your -- at your leisure to move through it.

So do we have those copies made? Let's go ahead and pass those out.

Is the verdict form attached to those, also?

LAW CLERK: It's also stapled.

THE COURT: It's a separate -- separate document? Okay.

All right. You should have a copy of the Court's charge, which is a rather thick stack, and then you should have a copy of the verdict form. Do you find both of those? I believe he's passing out the verdict form now.

All right. I'm going to -- let's just look at the verdict form first. I'll just cut to sort of the bottom line. These are the questions that you're going to be answering in light of the legal instructions that I'm going to be giving you in a moment.

But we'll go to the end of the chapter first and let you see where -- where you're going to end up, and then we'll go back and go through all of the legal instructions. But, basically, you're going to have three or four questions to answer.

The first question is: Did VirnetX prove by a preponderance of the evidence that Microsoft infringes certain claims of the '135 patent and certain claims of the '180 patent as listed there?

Then if you'll look on the next page, the top of the page, there's sort of a chart, and it has three columns; Column 1 dealing with infringement; Column 2 with willfulness; and Column 3 with invalidity.

And then down the left-hand side, you'll see the '135 patent and the three asserted claims; the '180 patent and the eight asserted claims underneath it.

So that first question, you would answer in Column 1, and that question is: Did VirnetX prove by a preponderance of the evidence that Microsoft infringes, and then it lists all of those claims of the '135 patent and the '180 patent.

And for the ones you find -- if you find infringement, then you would write yes in that blank. If you do not find infringement, then you would write no.

Then going back to Page -- the first page of the verdict form, you'll see Question No. 2: Of the claims that you have found infringed, in other words, the ones that you answered yes to, if any, did VirnetX prove by clear and convincing evidence that Microsoft's infringement was willful? And then an instruction to answer in Column 2.

So go back to that second page. For each one that you've answered yes to in Column 1, then you will answer either yes or no in Column 2 as to willfulness.

Then the third question is: Did Microsoft prove by clear and convincing evidence that any of the listed claims of the following patents are invalid?

And, again, if you find the claim invalid, answer yes; otherwise, answer no in Column 3.

And, again, on Column 3, you would answer yes or no for each claim.

Now, after you've answered those first three questions, then you have an instruction. If you have found that any claim -- any claim infringed and valid, answer Question 4; otherwise, do not answer Question 4.

So if you've found any claim to have been infringed and that it was not invalid, in other words, you answered yes to infringement for that claim and no to invalidity for that claim, then you would answer Question No. 4, which is the damages question.

And it asks: What sum of money, if paid now in cash, do you find, from a preponderance of the evidence, would fairly and reasonably compensate VirnetX for Microsoft's infringement of the following patents?

First, as to the '135 patent, and then for the '180 patent and a dollar sign and a place for your answer and then a place at the bottom for your jury foreperson to sign and date the verdict form.

Now, that's the end of the chapter, as I said. Now we'll go back through the detailed instructions. Some of these you've heard earlier and will be a repeat, but just please bear with me as we go through them.

Members of the Jury: You have now heard all of the evidence in this case. I'm now going to instruct you about the law which you must apply. It is your duty to follow the law as I give it to you.

On the other hand, you, the jury, are the judges of the facts. Do not consider any statement that I may have made during the trial or may make during these instructions as any indication that I have any opinion about the facts of this case.

After I instruct you on the law, the attorneys will have an opportunity to present their closing arguments. Again, the statements of the -- and arguments of the attorneys are not evidence and are not instructions on the law. They are only intended to assist you in understanding the evidence and the parties' contentions.

Again, as I told you at the beginning, the evidence will come -- is what you heard from the witness stand that was admitted into evidence and the documents and exhibits that were admitted.

Now, when you come to the questions, answer them from the facts as you find them. Do not decide who you think should win and then answer the questions accordingly. Your answers and your verdict must be unanimous.

In determining whether any fact has been proved in this case, you may, unless otherwise instructed, consider the testimony of all witnesses, regardless of who may have called them, and all exhibits received in evidence, regardless of who may have produced them.

Now, regarding considering witnesses' testimony, again, you, the jurors, are the sole judges of the credibility of all witnesses and the weight and effect of all evidence.

By the Court allowing testimony or other evidence to be introduced over the objection of an attorney, the Court did not indicate any opinion as to the weight or effect of such evidence.

When the Court sustained an objection to a question addressed to a witness, you must disregard the question entirely and may draw no inference from the wording of it or speculate as to what the witness would have testified to if he or she had been permitted to answer the question.

At times during the trial, it was necessary for the Court to talk with the lawyers here at the bench out of your hearing or by calling a recess. We met because often during a trial something comes up that does not involve the jury. You should not speculate on what was discussed during those times.

In determining the weight to give the testimony of a witness, you should ask yourself whether there was evidence tending to prove that the witness testified falsely concerning some important fact or whether there was evidence that at some other time, the witness said or did something or failed to say or do something that was different from the testimony the witness gave before you during the trial.

You should, of course, keep in mind that a simple mistake by a witness does not necessarily mean that the witness was not telling the truth as he or she remembers it, because people may forget some things or remember other things inaccurately.

So if a witness has made a misstatement, you need to consider whether that misstatement was an intentional falsehood or simply an innocent lapse of memory, and the significance of that may depend on whether it has to do with an important fact or only with some unimportant detail.

Now, with regard to examining the evidence, certain testimony in this case has been presented to you through a deposition. As I instructed you during the trial, a deposition is the sworn, recorded answers to questions asked of a witness in advance of trial.

Under some circumstances, the witness cannot be present to testify from the witness stand and the witness's testimony may be presented under oath in the form of a deposition.

Sometime before this trial, attorneys representing the parties in this case questioned this witness under oath. A court reporter was present and recorded the testimony.

This deposition testimony is entitled to the same consideration and is to be judged by you, as to credibility and weight, and otherwise considered by you, insofar as possible, the same as if the witness had been present and had testified from the witness stand in open court.

While you should consider all -- only the evidence in this case, you are permitted to draw such reasonable inferences from the testimony and exhibits as you feel are justified in the light of common experience.

In other words, you may make deductions and reach conclusions that reason and common sense leads you to draw from the facts that have been established by the testimony and in the case.

Unless you are instructed otherwise, the testimony of a single witness may be sufficient to prove any fact even if a greater number of witnesses may have testified to the contrary if, after considering all of the other evidence, you believe that single witness.

There are two types of evidence that you may consider in properly finding the truth as to the facts of the case.

One is the direct evidence, such as the testimony of an eyewitness.

The other is indirect or circumstantial evidence; that is, the proof of a chain of circumstances that indicates the existence or non-existence of certain other facts.

As a general rule, the law makes no distinction between direct and circumstantial evidence, but simply requires that you find the facts from a preponderance of all the evidence, both direct and circumstantial.

The parties may have stipulated or agreed to some facts in this case. When the lawyers on both sides stipulate to the existence of a fact, you must, unless otherwise instructed, accept the stipulation as evidence and regard that fact as proved.

Now, with regard to expert witnesses, when the knowledge of a technical subject matter may be helpful to the jury, a person who has special training or experience in that technical field is called an expert witness and is permitted to state his or her opinion on those technical matters.

However, you are not required to accept that opinion. As with any other witness, it is up to you to decide whether to rely upon it. In deciding whether to accept or rely upon the opinion of an expert witness, you may consider any bias of the witness.

Now, with regard to the contentions of the parties, I'm going to first give you a brief summary of each side's contentions in this case, and I will then tell you what each side must prove to win on these issues.

Plaintiff, VirnetX, contends that the Defendant, Microsoft Corporation, is directly infringing Claims 1, 10, and 12 of the '135 patent and Claims 1, 4, 15, 17, 20, 31, 33, and 35 of the '180 patent by making, using, selling, offering to sell, or importing into the United States patented systems or apparatuses or by using Microsoft's accused software to perform the patented methods.

These claims have been referred to as the asserted claims, and these patents have been referred as the patents-in-suit.

VirnetX also contends that Microsoft is inducing direct infringement of the '135 patent and contributing to direct infringement of the '135 patent by others who make or use the patented systems or perform the patented methods.

VirnetX also contends that Microsoft is inducing direct infringement of the '180 patent by others who make or use the patented apparatuses or perform the patented methods with Microsoft's accused software products.

VirnetX also claims that Microsoft has infringed the '135 and '180 patents willfully. That's the second question, as you'll recall from the verdict form. And VirnetX is seeking damages for Microsoft's alleged infringement.

In response to VirnetX's contentions, Microsoft contends that it is not infringing any of the asserted claims, whether willfully or otherwise.

Microsoft also contends that the asserted claims are invalid as being anticipated by or obvious in light of the prior art. Microsoft also contends that VirnetX is not entitled to any damages.

Now, with regard to the burdens of proof, we visited about this the first day.

VirnetX, in asserting infringement of the asserted claims of the '135 and '180 patents, has the burden of proving such infringement by a preponderance of the evidence.

Preponderance of the evidence means evidence that persuades you that a claim is more likely true than not true.

In determining whether any fact has been proved by a preponderance of the evidence, you may, unless otherwise instructed, consider the stipulations, the testimony of all the witnesses, regardless of who may have called them, and all the exhibits received into evidence regardless of who may have produced them.

If the proof establishes that VirnetX's infringement claims are more likely true than not true, then you should find for VirnetX as to that claim.

If you find that Microsoft infringed one or more of the asserted claims of the '135 and '180 patents, then as a separate question, VirnetX has the burden of proving its additional contention that the infringement was willful by clear and convincing evidence.

Microsoft has the burden of proving invalidity by clear and convincing evidence.

Clear and convincing evidence means evidence that produces in your mind a firm belief or conviction as to the matter at issue.

In determining whether any fact has been proved by clear and convincing evidence, you may, unless otherwise instructed, again, consider the stipulations all the witnesses' testimony, regardless of who may have called them, and all of the exhibits admitted into evidence, regardless of who may have produced them.

Although proof to an absolute certainty is not required, the clear-and-convincing-evidence standard requires a greater degree of persuasion than is necessary for the preponderance-of-the-evidence standard. If the proof establishes in your mind a firm belief or conviction, then the standard has been met.

01:23 So if you'll look back at the verdict form, the three -- first three questions and on the second page, the Columns 1, 2, and 3, the first column, infringement, that's under the preponderance-of-the-evidence standard.

01:25 The next two columns: Willfulness and invalidity, that's under the clear-and-convincing standard.

01:25 Everybody follow that?

01:25 Okay. Now, a glossary of patent terms is contained in Appendix B to this charge. I'm not going to read through all of those. They're there for your reference.

01:25 You'll see them over as the last two pages -- most of those have been testified to and explained, but that's there for your reference, and you should read them. They are part of the charge.

All right. Now, with regard to the claims of the patents-in-suit, the claims of a patent are numbered sentences at the end of the patent.

The claims describe the invention made by the inventor and describe what the patent owner owns and what the owner may prevent others from doing. Claims may describe products, such as machines or chemical compounds or processes for making or using a product.

Claims are usually divided into parts or steps called limitations or elements. For example, a claim that covers the invention of a table may recite the tabletop, four legs, and the glue that secures the legs on the tabletop. The tabletop, the legs, and the glue are each a separate limitation or element of the claim.

Now, there are two types of claims. This case involves independent claims and dependent claims.

An independent claim sets forth all the requirements that must be met in order to be covered by that claim. Thus, it is not necessary to look at any other claim to determine what an independent claim covers.

In this case, Claims 1 and 10 of the '135 patent and Claims 1, 17, and 33 of the '180 patent are each independent claims.

The other claims being asserted in this case are dependent claims. A dependent claim does not itself recite all of the requirements of the claim but refers to another claim for some of its requirements.

In this way, the claim depends on another claim.

The law considers a dependent claim to incorporate all of the requirements of the claims to which it refers. The dependent claim then adds its own additional requirements.

To determine what a dependent claim covers, it is necessary to look at both the dependent claim and any other claims to which it refers. A product or method that meets all of the requirements of both the dependent claim and the claims to which it refers is covered by that dependent claim.

Construction of the claims.

In deciding whether a claim has been infringed, the first step is to understand the meaning of the words used in the patent claims.

It is my job as judge to determine what the patent claims mean and to instruct you about that meaning. You must accept the meanings I give you and use those meanings when you decide whether or not the patent claims are infringed and whether or not they are invalid.

I have interpreted the meaning of some of the language in the patent claims involved in this case. My interpretation of those claims appears in Appendix A to this charge.

The claim language I have not interpreted for you in Appendix A is to be given its ordinary and accustomed meaning as understood by one of skill in the art.

Now, with regard to infringement, any person or business entity that, without the patent owner's permission, makes, uses, sells, or offers to sell a device or practices a method, that is covered by at least one claim of a patent before the patent expires infringes the patent.

A patent owner has the right to stop others from infringing the patent claims during the life of the patent.

In this case, VirnetX asserts that Microsoft has infringed the asserted claims. VirnetX has the burden of proving infringement by a preponderance of the evidence.

Only the claims of a patent may be infringed. You must compare each of the asserted claims, as I have defined them, to the accused acts of infringement and determine whether or not there is infringement.

You must not compare the accused products or methods with any specific example set out in the patents. The only correct comparison is with the language of the claim itself with the meanings I have given you.

In order to prove infringement, VirnetX must prove that the requirements for one or more of these types of infringement are met by a preponderance of the evidence; that is, that it's more likely not, that all of the requirements of one or more of each of these types of infringement have been proved.

You must consider each claim individually and must reach your decision as to each assertion of infringement based on my instructions about the meaning and scope of the claims, the legal requirements for infringement, and the evidence presented to you by the parties.

In this case, there are three possible ways that a claim may be infringed: The first is direct infringement; the second is active inducement; and the third is contributory infringement.

VirnetX has alleged that Microsoft directly infringes the asserted claims.

In addition, VirnetX has alleged that customers of Microsoft directly infringe the asserted claims and that Microsoft is liable for actively inducing or contributing to that direct infringement by those customers.

I will now explain each of the types of infringement in more detail.

The first is direct Infringement. If any person makes, uses, sells, or offers to sell what is covered by the claims of a patent without the patent owner's permission, that person is said to infringe the patent. This type of infringement is also called direct infringement.

To determine direct infringement, you must compare the accused product or method with each of the asserted claims of the patents-in-suit using my instructions as to the meaning of the patent claims.

A patent claim is directly infringed only if the accused product or method includes each and every element in that patent claim. If the accused product or method does not contain one or more of the limitations recited in a claim, then that product or method does not directly infringe that claim.

An accused product infringes a claim if it is reasonably capable of satisfying the claim elements, even though it may also be capable of non-infringing modes of operation.

If you find that the accused product or method includes each element or step of the claim, then the product or method infringes the claim even if such product or method contains additional elements or steps that are not recited in the claim.

A person can directly infringe a patent without knowing that what it is doing is an infringement of the patent.

It may also directly infringe, even though, in good faith, it believes that what it is doing is not an infringement of any patent, and even if it did not know of the patent infringement -- even if it did not know of the patent, infringement does not require proof that the person copied a product or the patent.

You must consider each of the asserted claims of the patents-in-suit individually and decide whether making, selling, or using the accused apparatuses or performing the accused methods infringes that claim.

You must be certain to compare such accused apparatus or method with each claim that such apparatus or method is alleged to infringe. Such accused apparatus or method should be compared to the limitations recited in the patent claims, not to -- and not to any preferred or commercial embodiment of the claimed invention.

Taking each asserted claim of the '135 and '180 patents separately, if you find that VirnetX has proved by a preponderance of the evidence that each and every limitation of that claim is present in the accused product or method, then you must find that such product or method infringes the claim.

A claim limitation may be directly infringed in one of two ways: Either literally or under the Doctrine of Equivalents.

Literal infringement.

A claim limitation is literally met if it exists in the accused product or method just as it is described in the claim language, either as I have explained that language to you, or if I did not explain it, as it would be understood by one of skill in the art.

The second way is under the Doctrine of Equivalents. A claim limitation is present in an accused product or method under the Doctrine of Equivalents if the differences between the claim limitation and a comparable element of the accused product or method are insubstantial.

One way to determine whether a difference is insubstantial is to look at whether the accused product or method performs substantially the same function in substantially the same way to achieve substantially the same result as the claimed invention.

You may also consider whether, at the time of the alleged infringement, a person having ordinary skill in the field of technology of the patent would have known of the interchangeability of the alternative feature and the unmet requirement of the claim.

Interchangeability at the present time is not sufficient in order for the features to be considered to be interchangeable; rather, the interchangeability of the two features must have been known to persons of ordinary skill in the field of technology at the time the infringement began.

Thus, the inventor need not have foreseen and the patent need not describe all potential equivalents to the invention covered by the claims.

Also, slight changes in technique or improvements made possible by technology developed after the patent application is filed may still be considered equivalent for the purposes of the Doctrine of Equivalents.

Now, with regard to inducement, VirnetX alleges that Microsoft is also liable for infringement by actively inducing others to directly infringe the '135 and '180 patents.

As with direct infringement, you must determine whether there has been active inducement on a claim-by-claim basis.

A person is liable for active inducement of a claim only if:

(1) the person takes action during the time the patent is in force, which encourages acts someone else;

And (2) the encouraged acts constitute direct infringement of that claim;

And (3) the person is aware of the patent and knows or should have known that the encouraged acts constitute infringement of that patent;

And (4) the person has an intent to cause the encouraged acts;

And (5) the encouraged acts are actually carried out by someone else.

In order to prove active inducement, VirnetX must prove that each of the above requirements is met. Further proof of each element must be by a preponderance of the evidence; i.e., that it is likely than not that each of the above requirements has been met.

In considering whether Microsoft has induced infringement by others, you may consider all the circumstances, including whether or not Microsoft obtained the advice of a competent lawyer, whether or not Microsoft knew of the patents when designing and manufacturing its products, and whether or not Microsoft removed or diminished the allegedly infringing features.

You may not assume that merely because Microsoft did not obtain an opinion of counsel, the opinion would have been unfavorable.

Intent to cause the acts that constitute direct infringement may be demonstrated by evidence of active steps taken to encourage direct infringement, such as advertising an infringing use or instructing how to engage in an infringing use.

In order to establish active inducement of infringement, it is not sufficient that the accused infringer was aware of the acts that allegedly constitute the direct infringement; rather, you must find specifically that the inducer intended to cause the acts that constitute the direct infringement and must have known or should have known that its action would cause the direct infringement.

If you do not find that the accused infringer specifically meets these intent requirements, then you must find that the accused infringer has not induced the alleged infringement.

Next is contributory infringement.

VirnetX also alleges that Microsoft is

liable for contributory infringement by contributing to the direct infringement of the '135 patent by another. As with direct infringement, you must determine whether there has been contributory infringement on a claim-by-claim basis.

It is not necessary to show that Microsoft has directly infringed as long as you find that someone has directly infringed. If there is no direct infringement by anyone, Microsoft cannot have contributed to the infringement of the patent.

If you find someone has directly infringed the '135 patent, then contributory infringement exists if VirnetX proves by a preponderance of the evidence that:

(1) Microsoft sold, offered for sale, or imported;

(2) a material component of the product or material component used in practicing the patented method, which can be software, that is not a staple article of commerce suitable for substantial non-infringing use;

(3) with knowledge that the component was especially made or adapted for use in an infringing manner.

A staple article of commerce suitable for substantial non-infringing use is something that has uses other than a component of the product or patented method.

A substantial non-infringing use is one that is not occasional, farfetched, impractical, experimental, or hypothetical.

In determining whether or not the component is a staple article of commerce suitable for non-infringing use, you should focus on whether the component itself, not the product in which the component is embedded, is or is not suitable for substantial non-infringing use.

Whether the product in which the component is embedded is or is not suitable for substantial infringing use is not relevant.

Now, next is willful infringement. Again, willfulness is the second question, and you'll place your answers in Column 2 based on the clear-and-convincing-evidence standard.

VirnetX contends that Microsoft has willfully infringed the asserted claims. If you find, on the basis of the evidence and the law, as I have explained it, that Microsoft directly or indirectly infringes at least one of the asserted claims, then you must decide whether or not that infringement was willful.

Willfulness is not relevant to your decision of whether or not there is infringement. It is relevant only to the amount of damages, if any, and may, in certain circumstances, entitle the patent owner to increased damages.

But it would be my job to decide whether to award increased damages to a patent owner, after you have rendered a verdict. Therefore, you should not consider willful infringement in making your damage award, if any.

To prove willfulness, a patent owner must prove by clear and convincing evidence that the accused infringer acted with reckless disregard to the claims of the asserted patent.

Willfulness requires you to determine three things:

First, that the accused infringer was aware of the asserted patent;

Second, that the alleged infringer acted despite an objectively high likelihood that its actions infringed a valid patent;

And third, that this objectively high risk was either known or so obvious that it should have been known to the alleged infringer.

In deciding whether or not the alleged infringer committed willful infringement, you must consider all of the facts, including:

(1) whether or not the alleged infringer possessed a reasonable basis to believe that it has a substantial defense to infringement and reasonably believed that the defense would be successful if litigated, including the defense that the patent is invalid;

And (2) whether or not the alleged infringer made a good faith effort to avoid infringing the patent; for example, the alleged infringer took remedial action upon learning of the patent by ceasing infringing activity or attempting to design around the patent.

Now that covers infringement and willfulness.

Now my instructions regarding invalidity. That's the third question that you'll answer in Column 3, and that standard of proof is clear and convincing evidence.

Microsoft has challenged the validity of all of the asserted claims of the '135 and '180 patents on a number of different grounds. Microsoft must prove that a patent claim is invalid by clear and convincing evidence.

An issued patent is accorded a presumption of validity based on the presumption that the United States Patent & Trademark Office acted correctly in issuing a patent.

For a patent to be valid, the invention claimed in the patent must be new, useful, and obvious. A patent cannot take away from people their right to use what was known or what would have been obvious when the invention was made.

In addition, the patent must comply with certain statutory requirements of disclosure.

I will now explain to you in some detail Microsoft's grounds for invalidity. In making your determination as to invalidity, you should consider each claim and each ground for invalidity separately.

The first is anticipation. And you've heard testimony about all of these during the course of the trial from both sides.

Microsoft contends that all of the asserted claims are invalid for being anticipated by prior art. Microsoft bears the burden of proof of establishing anticipation by clear and convincing evidence.

A patent claim is invalid if the claimed invention is not new. For a claim to be invalid on the basis of anticipation because it is not new, all of its requirements must be present in a single previous device or method or described in a single previous publication or patent. We call these things prior art.

Microsoft must prove by clear and convincing evidence that these items are prior art. The description in a reference does not have to be in the same words as the claim, but all the requirements of the claim must be there, either stated expressly or necessarily implied or inherent in the level of ordinary skill in the field of technology of the patent so that someone of ordinary skill in the field of technology of the patent, looking at that one reference would be able to make and use the claimed invention.

Something is inherent in an item of prior art if it is always present in the prior art or always results from the practice of the prior art.

Inherency may not be established by probabilities or possibilities. The mere fact that a certain thing may coincidentally result from a given set of circumstances is not sufficient.

A party claiming anticipation by inherency must show that the elements of the claim are always present in the prior art or always result from the practice of the prior art. You may not combine one or more items of prior art to make out an anticipation.

Let me now instruct you on two principles of patent law pertaining to the making of an invention. Conception and reduction to practice are those two areas.

Conception is the mental part of an invention; in essence, the formation in one's mind of the inventor of a definite and permanent idea of the complete and operative invention as it is hereafter to be applied in practice.

Conception of an invention is complete when the idea is so clearly defined in the inventor's mind that a person of ordinary skill in the field of the technology would be able to reduce the invention to practice without extensive research or experimentation.

Conception may be proved when the invention is shown in its complete form by drawings, disclosure to another person or other forms of evidence presented at trial.

The second, a claimed invention is reduced to practice when it has been tested sufficiently to show that it will work for its intended purpose.

An invention may be reduced to practice even if the inventor has not made or tested a prototype of the invention. The invention may be reduced to practice by being fully described in a filed patent application.

Anticipation by public knowledge or use by another. I will now describe the specific requirements for the prior art categories relied on by Microsoft in this case.

A patent claim is invalid if the invention recited in that claim was publicly known or used in the United States by someone other than the inventor before the patent applicant invented it or more than one year before the United States patent application was filed.

For the '135 patent, the parties agree that the invention date was February 15, 2000.

For the '180 patent, the parties agree that the invention date was April 26, 2000.

A prior public use by another may anticipate a patent claim even if the use was accidental or was not appreciated by the other person. Thus, a prior public use may anticipate an invention even if the user did not intend to use the invention or even realize he or she had done so.

Private or secret knowledge, such as knowledge confidentially discussed within a small group, is not enough to invalidate a prior -- invalidate a patent claim.

Now anticipation by a printed publication.

A patent claim is invalid if the invention defined by that claim was described in a printed publication anywhere in the world before it was invented by the patent applicant or more than one year prior to the filing date of the United States patent application.

The effective filing date of the application of the '135 patent is February 15, 2000.

The effective filing date of the application for the '180 patent is April 26, 2000.

Printed publications may include issued patents, as well as articles, treatises, and other written materials.

A printed publication or patent will not be an anticipation unless it contains a description of the invention covered by the patent claims that is sufficiently detailed to teach a skilled person how to make and use the invention without undue experimentation.

Factors to be considered in determining whether a disclosure would require undue experimentation include:

(1) the quantity of the experimentation necessary;

(2) the amount of direct -- the amount of direction or guidance disclosed in the printed publication or patent;

(3) the presence or absence of working examples in the printed publication or patent;

(4) the nature of the invention;

(5) the state of the prior art;

(6) the relative skill of those in the art;

(7) the predictability of the art;

And (8) the breadth of the claims.

A printed publication must be reasonably accessible to those members of the public who would be interested in its contents. It is not necessary that the printed publication be available to every member of the public. The date that a printed publication becomes prior art is the date that it becomes available to the public.

So long as the printed publication was available to the public, the form in which the information was recorded is unimportant. The information must, however, have been maintained in some permanent form, such as printed or typed pages, magnetic tape, microfilm, photographs, or photocopies.

Now, anticipation by prior sale or offer for sale.

The sale or offer for sale in the United States of a product may be prior art to a patent claim covering the product or a method of making the product if the product or method was sold or offered for sale in the United States more than one year before the application for the patent was filed.

This is known as the on-sale bar. The date of the invention for the patent claims is irrelevant to this category of prior art.

In order for there to be an offer for sale, two requirements must be met.

First, the product have been the subject of a commercial offer for sale in the United States. Even a single offer sale to a single customer may be a commercial offer, even if the customer does not accept the offer.

The on-sale bar is not limited to sales by the inventor but may result from sales or offers for sale by a third party that anticipate the invention.

Second, the product must be ready for patenting. This can be satisfied in at least two ways:

(1) by proof of reduction to practice; that is, the alleged invention worked as actually intended before the critical date;

Or (2) by proof that prior to the critical date, the inventor had prepared drawings or other descriptions of the invention that were sufficiently specific to enable a person skilled in the art to practice the invention.

The product may be ready for patenting even if it is not ready for commercial production or has not been technically perfected.

Corroboration of oral testimony.

Oral testimony alone is insufficient to prove prior invention or that something is prior art or that a particular event or reference occurred before the filing date of the patents-in-suit.

A party must provide evidence that corroborates any oral testimony, especially where the oral testimony comes from an interested witness or a witness testifying on behalf of an interested party.

This includes any individual or company testifying that his or her -- or its invention predates the patents-in-suit and also includes a patent owner seeking to prove an earlier date of invention than the effective -- than the effective filing date stated on the face of the patent.

Documentary or physical evidence that is made contemporaneously with the inventive process provides the most reliable proof that the testimony has been corroborated, but corroborating evidence may also consist of testimony of a witness, other than an inventor, to the actual reduction to practice, or it may consist of evidence of surrounding facts and circumstances independent of information received from the inventor.

If you find that the party has not corroborated the oral testimony with other evidence, you are not permitted to find that the subject of the oral testimony qualifies as prior art or supports a prior date of invention.

Next is the defense of obviousness.

Not all innovations are patentable. A patent claim is invalid for obviousness if the claimed invention as a whole would have been obvious to one having ordinary skill in view of all the prior art at the time the invention was made.

The issue is not whether the claimed invention would have been obvious to you as a layman, to me as a judge, or to a genius in the art, but whether it would have been obvious to one of ordinary skill in the art at the time it was made.

Microsoft bears the burden of proving this defense by clear and convincing evidence.

You must not use hindsight when comparing the prior art to the invention for obviousness. You should consider only what was known before the invention was made. You may not judge the invention in light of present-day knowledge or by what you learned from or about the claimed invention during trial.

In placing yourself in the shoes of one of ordinary skill in the art at the time that the invention was made, you may consider whether such a person would have been motivated to combine the prior art references in order to arrive at the claimed invention.

First, you must decide the level of ordinary skill in the field that someone would have had at the time the claimed invention was made.

Second, you must decide the scope and content of the prior art put into evidence in this case.

Third, you must decide the differences, if any, that existed between the claimed invention and the prior art.

Finally, you should consider any additional considerations relating to the obviousness or non-obviousness of the invention.

I will now describe in detail the specific determinations you must make.

These instructions often refer to a person of ordinary skill in the art. It is up to you to decide the level of ordinary skill in the field of the claimed inventions.

You should consider all the evidence introduced at trial in making this decision, including:

(1) the levels of education and experience of persons working in the field;

(2) the types of problems encountered in the field;

And (3) the sophistication of the technology.

VirnetX contends a person of ordinary skill in the art would have a master's degree in computer science or computer engineering or in a related field, as well as approximately two years of experience in computer networking and in security with respect to computer networks, including actual experience with networking protocols, as well as the security of those protocols.

Microsoft contends that the level of ordinary skill in the field was a person with a bachelor's degree in computer engineering or computer science or equivalent and two to three years experience with data networks.

Now, with regard to the scope and content of the prior art, in determining whether or not the invention is valid, you must determine the scope and content of the prior art at the time the invention was made.

You must decide whether the specific references relied upon by Microsoft in this case are prior art to the invention described in the asserted claims of the patents-in-suit.

Prior art includes previous devices, articles, and methods that were publicly used or offered for sale and printed publications or patents that disclose the invention or elements of the invention.

Once you decide whether or not specific references are prior art, you must also decide what those references would have disclosed or taught to one having ordinary skill in the field of the technology of the patent at the time the invention was made.

In order for a reference to be relevant, the reference must be within the field of the inventor's endeavor, or if it is from another field of endeavor, the reference must be reasonably related to the particular problem or issue the inventor faced or addressed when making the inventions described in the asserted claims of the patents-in-suit.

A reference from a field of endeavor,

other than the inventor's, is reasonably related to the problem or issues the inventors faced if the reference is one which, because of the matter -- because of the matter with which the reference deals, logically would have commended itself to the attention of the inventors when considering the problems or issues they faced.

It is for you to decide what the problems or issues were that the inventors faced at the time the inventions in the asserted claims were made.

Now the differences over the prior art.

The next question you must answer in determining whether or not the invention was obvious at the time it was made is what differences there are, if any, between the prior art and the patented invention.

In analyzing this issue, do not focus on the differences between the prior art and the invention because the test is not whether there are differences; rather, the test is whether or not the invention, taken as a whole, would have been obvious to one having ordinary skill in view of all the prior art at the time the invention was made.

If you conclude that the prior art discloses all the elements of the asserted claims, but those elements are in separate items, you must then consider whether or not it would have been obvious to combine those items.

A claim is not obvious merely because all of the elements of that claim already existed. One way to decide whether one of ordinary skill in the art would combine what is described in various items of prior art is whether there is some teaching, suggestion, or motivation in the prior art for a skilled person to make the combination covered by the patent claims. Motivation can be implicit or explicit.

In considering whether a claimed combination of prior art elements is obvious, you must consider whether the improvement is more than the predictable use of prior art elements according to their established functions.

When a patent simply arranges old elements with each performing the same function it had been known to perform and yields no more than one would expect from such an arrangement, the combination is obvious.

It is common sense that familiar items may have obvious uses beyond their primary purposes, and a person of ordinary skill often will be able to teach -- to fit the teachings of multiple patents together like the pieces of a puzzle. Multiple references in the prior art can be combined to show that a claim is obvious.

Any need or problem known in the field and addressed by the patent can be -- can provide a reason for combining the elements in the manner claimed.

To determine whether there was an apparent reason to combine the known elements in the way a patent claims, you can look to interrelated teachings of multiple patents, to the effects of demands known to the design community or present in the marketplace, and to the background knowledge possessed by a person of ordinary skill in the art.

Neither the particular motivation nor the alleged purpose of the patentee controls. One of ordinary skill in the art is not confined only to prior art that attempts to solve the same problem as the patent claim.

Teachings, suggestions, and motivations may also be found within the knowledge of a person with ordinary skill in the art, including inferences and creative steps that a person of ordinary skill in the art would employ.

Additionally, teachings, suggestions, and motivations may found in the nature of the problems solved by the claimed invention. The fact that a combination was obvious to try may demonstrate that the combination itself was obvious.

Additional considerations.

The next question you must answer in determining whether or not the invention was obvious at the time it was made is what evidence there is, if any, of additional considerations relating to the obviousness or non-obviousness of the invention.

You may consider in your analysis any evidence about the following factors, and then it lists ten separate factors that are additional considerations there, and if there's no objection, I'll just leave those to the jury for reading.

To be relevant to your determination of obviousness, any of these secondary considerations must have a connection or nexus to the claimed invention set forth in the patent claims.

If a secondary consideration is unrelated to the claimed invention but is, instead, attributable to something else, such as innovative marketing, then you should not consider it relevant to your obviousness determination.

So that concludes the instructions on the first three questions to be answered in Columns 1, 2, and 3. The next question is the damage question, and I'll now give you instructions about that.

By instructing you on damages, however, I am not suggesting which party should win this case on any issue. If you find that Microsoft infringed any valid asserted claim of the '135 and '180 patents, you must then determine the amount of money damages to be awarded to VirnetX to compensate it for the infringement.

VirnetX seeks patent damages in the form of a reasonable royalty. Generally, a reasonable royalty is defined by the patent laws as the reasonable amount that someone wanting to use the patented invention would expect to pay to the patent owner and the owner should expect to receive.

A damages award should put the patent owner in approximately the financial position it would have been in had the infringement not occurred. You may not add anything -- you may not add anything to the amount of damages to punish the infringer or to set an example.

VirnetX has the burden to persuade you by a preponderance of the evidence that it has suffered the damages it seeks. While VirnetX is not required to prove damages with mathematical precision, it must prove them with reasonable certainty. The patent owner is not entitled to damages that are remote or speculative.

Now, reasonable royalty.

A royalty in the amount -- a royalty is the amount of money a licensee pays to a patent owner to make, use, or sell the patented invention.

A reasonable royalty is the amount of money a willing patent owner and a willing prospective licensee would have agreed upon at the time of the infringement for a license to make the invention.

It is the royalty that would have resulted from an arm's-length negotiation between a willing licensor and a willing licensee, assuming that both parties understood the patent to be valid and infringed and that the licensee would respect the patent.

Unlike a real world negotiation, in the hypothetical negotiation, all parties are presumed to know that the patent is infringed and is valid.

In making your determination about the amount of a reasonable royalty, it is important that you focus on the time period when the infringer first infringed the patent and the facts that existed at that time.

Your determination does not depend on the actual willingness of the parties to this lawsuit to engage in such negotiations. Your focus should be on what the parties' expectations would have been had they entered negotiations for royalties at the time of the infringing activity.

The infringer's actual profits may or may not bear on the reasonableness of an award based on a reasonable royalty.

Reasonable royalty factors.

In deciding what is a reasonable royalty, you may consider the factors that the patent owner and the alleged infringer would consider in setting the amount the alleged infringer should pay.

Listed below are a number of factors you may consider. This is not every possible factor, but it will give you an idea of the kinds of things to consider in setting a reasonable royalty.

You've heard various ones testified about during this trial. There are 15 of them listed there for you, and unless, there's an objection, I will just refer those to you for your reading.

No one of these factors is dispositive, and you can and should consider the evidence that has been presented to you in this case on each of these factors. The attorneys, in their arguments, will focus on the factors that they deem raised by the evidence and most important.

The framework which you should use in determining a reasonable royalty is, again, a hypothetical negotiation between normally prudent business people.

Now, let me give you some instructions for your deliberations.

You must perform your duties as jurors without bias or prejudice as to any party. The law does not permit you to be controlled by sympathy, prejudice, or public opinion.

All parties expect that you will carefully and impartially consider all the evidence, follow the law, as it is now being given to you, and reach a just verdict, regardless of the consequences.

You should consider and decide this case as a dispute between persons of equal standing in the community, of equal worth, and holding the same or similar stations in life.

A corporation is entitled to the same fair trial as a private individual. All persons, including corporations, and other organizations stand equal before the law, regardless of size or who owns them, and are to be treated as equals.

When you retire to the jury room to deliberate on your verdict, you may take this charge with you, as well as the exhibits which the Court has admitted into evidence.

You should first select your foreperson and then begin your deliberations.

If you recess during your deliberations, follow all of the instructions that the Court has given you about and on your conduct during the trial.

After you have reached your verdict, your foreperson is to fill in on the form your answers to the four questions that have been asked of you. Do not reveal your answers until such time as you are discharged, unless otherwise directed by me.

You must never disclose to anyone, not even to me, your numerical division on any question.

Any notes that you may have taken during this trial are only aids to your memory. As I told you earlier, if your memory should differ from your notes, then you should rely on your memory, not on your notes. The notes are not evidence.

A juror who has not taken notes should rely on his or her independent recollection of the evidence and should not be unduly influenced by the notes of other jurors. Notes are not entitled to any greater weight than the recollection or impression of each juror about the testimony.

If you wish to communicate with me at any time, please give a written message or question to the court security officer, who will bring it to me. I will then respond as promptly as possible either in writing or having you brought into the courtroom so that I can address you orally.

I will always first disclose to the attorneys your question and my response before I answer your question.

After you have reached a verdict, you are not required to talk with anyone about the case unless the Court orders otherwise.

Now, the next sentence doesn't apply yet, because it says you are to retire to the jury room to begin your deliberations. But we're not going to do that yet, because you haven't heard the closing arguments.

But what I am going to do is give you a 15-minute break. I'm going to ask you to continue to follow my instructions. Even though you've heard the opening statements, all the evidence, the Court's charge, you still haven't heard the final closing arguments.

So I'm going to ask you not to discuss the case among yourselves or with anyone else, but just have a -- it's been a lengthy time of instruction for you. You've been sitting there for well over an hour, so we're going to take a 15-minute break.

When we come back, each side has been given one hour -- is that correct?

MR. CAWLEY: Yes, Your Honor.

THE COURT: One hour for closing argument.

So we're going to come back at 3:30, and that's going to push us until 5:30 until the argument is over.

Once the arguments are over, I'm going to dismiss you to the jury room, and I'm then going to ask you to select your jury foreperson, and then you will make a decision as to whether you would like to begin deliberations tonight for however long you wish or whether you would like to go home and come back in the morning and begin deliberations.

So I'll remind you of those instructions at the end of the case, but I just want to tell you that, because in all probability, you're going to be here until at least 5:30 to 6:00 o'clock tonight.

So if you need to notify any family members or -- now, did somebody have a child issue or not on this jury? I guess that was the last case.

Okay. If -- if anyone has any issues with that time or need to make arrangements to let anyone know, please do so during your break.

02:17 Again, as I've instructed you, I've allowed you to have your cell phones for purposes of coordinating with family and that type of thing. But, again, don't discuss the case in any phone calls that you might choose to make to let people know what your schedules are going to be.

02:17 I will allow you during this break, if you wish, to discuss between yourselves for scheduling purposes your collective thought as to whether you think you'd like to begin deliberating tonight or whether you'd like to come back in the morning.

02:17 But in making that, you're not to discuss the case, the merits, one way or the other; just from a tiredness standpoint or from a scheduling standpoint. You may discuss whether y'all have reached some collective decision as to whether you'd like to work for a little while tonight.

02:18 Once we get through with the arguments, you're going to be in charge. You can go home, come back in the morning. You can work for an hour tonight. You can work till midnight. You can do whatever you want to do. We're going to be at your pleasure.

02:18 You've been at everyone else's pleasure all week, and you're going to be in the driver's seat as soon as we're through with closing arguments.

So with that, please follow my instructions, and you are released to the jury room until 2:35. I'm sorry. That will be 3:35.

COURT SECURITY OFFICER: All rise.

(Recess.)

(Jury out.)

COURT SECURITY OFFICER: All rise.

THE COURT: Please be seated.

All right. Now, does someone want to withdraw a JMOL?

MR. CAWLEY: I do, Your Honor.

THE COURT: Okay.

MR. CAWLEY: I was reminded over the break by Mr. Bobrow that we, in fact, had had some e-mail exchange on the -- that issue about claim 7 of the '135 patent, and I requested that it be JMOL and they requested they withdraw it without prejudice, and it looks like we agreed to withdraw without prejudice.

THE COURT: Claim 7 is dismissed without prejudice.

MR. CAWLEY: We stand by that.

MR. CALDWELL: Thank you, Your Honor.

THE COURT: Thank you.

All right. Ready for the jury to be brought in?

02:38 MR. CAWLEY: Yes, sir. I would like to reserve 10 minutes for rebuttal.
02:38 THE COURT: All right. Bring the jury in, please.
02:39 (Jury in).
02:39 THE COURT: Please be seated.
02:39 All right, ladies of the jury, we're getting near the end now. So we're -- we've now made it all the way down to closing arguments which we're about to hear in just a moment.
02:39 Let me just inquire of you, did y'all have a chance to discuss whether you'd like to begin deliberations tonight or whether you would like to come back in the morning?
02:39 JUROR: Both.
02:39 THE COURT: Both. Okay. Begin tonight and work for a little while and then maybe come back in the morning is --
02:39 JUROR: We have one that needs to be home by 7:00.
02:39 THE COURT: Okay.
02:39 JUROR: So we thought we would work till 6:30.
02:39 THE COURT: Okay. Very good. Very good. You're working well together already. So, very good.

Thank you for your attention. Please bear with us and pay attention to the attorneys' closing arguments. And I know my instructions were very lengthy and somewhat overwhelming, but I promise you the attorneys will, just as they -- both sides have done throughout this case, they will bring the issues that the case is really -- that are dispositive into focus for you, point out the instructions that are important, and you'll have a -- have a good -- good sense when you go to the jury room.

So with that, Mr. Cawley, the Court will recognize you for purposes of closing argument.

MR. CAWLEY: Thank you, Your Honor.

When we first met two weeks ago for the jury selection, I suggested to you that every lawsuit is a story, and as this lawsuit has been tried, it's been occurring to me that what we heard is a lot like an old story that many of you may have heard.

It's a story about a mustard seed. And the story is that the mustard seed is the least of all the seeds, because it's so tiny. But the story goes that if you plant that tiny seed in a garden and you wait, if you wait until its time is right and its time comes, that that tiny seed can grow into a mighty tree. And the story concludes by telling us that when that happens, the birds of the air made nests in its branches.

The lawsuit is a story about a seed, a seed of an idea. You may remember that that seed first arose in war time for application on the battlefield. The United States was faced with a grave crisis involving scud missiles. Those were missiles that the Iraqi Army could bring out of hiding and, within 10 minutes, launch off into Israel. The United States had agreed to try and stop that.

They hired Mr. Gif Munger and Mr. Bob Short and a handful of other men to find a solution, and the solution they came up with was called the Global Hawk.

You'll remember that one of the unusual things about the Global Hawk system was that it used a commercially available satellite rather than a military satellite. A satellite that anyone who wanted to rent time on could use to broadcast television or radio or anything else.

And this presented a real problem for the military to be able to secure the communications that went from that satellite down to the ground. Without securing them, it was possible that someone on the ground, a hacker, a member of the enemy military might be able to intercept those communications and know what was about to happen.

Mr. Munger and Mr. Short and their team, therefore, came up with a way to secure those satellite communications so that any hackers on the ground would be locked out.

Now that set Mr. Munger to thinking. You heard him testify from the witness stand. This is the mid-to-late 1990s, and it began to occur to him that this was going to happen more and more frequently. That as communications around the world grew, cellular telephones, the normal telephone system, the internet, satellite communications, that it was going to become more and more common that the military would have to use publicly-available communications facilities.

He also began to observe that not only the military but that all of us were coming to depend on the communications through the internet, and not just to send our friends e-mail and to send out pictures of our grandchildren. But a lot of the commerce of our nation was being conducted over the internet, so Mr. Munger began to see that in terms of being part of our national security, to be able to secure communications on the internet.

He wrote a paper about that that he called the Aladdin paper because he saw a world where you could rub a magic lamp and get all kinds of communications abilities for the military and for others. And eventually his company, SAIC, entered into a contract with the CIA, and the purpose of this contract was to help the CIA find a way to easily, but safely and securely, communicate over the internet.

Mr. Bob Short -- Dr. Bob Short took the stand and explained to you that in doing research for that project that was called NetEraser, he and his team bought all the available software and hardware they could find that could be used in that time, 1998 and 1999, to set up a virtual private network.

Now everybody in the case agrees that Mr. Munger and Dr. Short didn't invent virtual private networks. Those were already available. And once they were set up, could already be used to send communications securely across the internet when they were doing this job for the CIA.

But what you did hear Mr. Short explain, standing right down here, at some length is how difficult it was to set up the virtual private networks that were available at that time period.

You saw him draw on this board on many pages of it with a red marker that showed you step after step the complicated procedures that had to be followed to set up a virtual private network. And although Microsoft told you, well, there were other ways to do it, we had other projects and documents like this Defendant's Exhibit 3021, when we examined them about it, we discovered that this supposedly easy way to do it has 25 pages of instructions. Again, an example of how difficult, how unwieldy, and how impractical the setup of virtual private networks were in the late 1990s.

But then these men who had been working on this problem, researching it, studying it for about six months, had a breakthrough. In their breakthrough they planted the seed.

You'll remember, they explained to you the vision that they had was that a remote user of a computer who wanted to communicate securely could click one key on the keypad and their computer would automatically use something called a DNS request. That DNS request would go to software on the sender's end that was part of the invention which would communicate back to the remote user the information necessary to set up the secure virtual private network.

Again, without having to do anything but the click of that one key, that computer would then communicate with other computers on the network which in turn had software that was part of the invention, and those computers would negotiate how the virtual private network would be set up. It would be just as secure as the virtual private network set up the old-fashioned, laborious way, but it could be done with one click of the key. And Dr. Short showed you that on the laptop computer that he had set up that you'll remember went out over the internet, came back into the courtroom through a completely different channel from Mr. Munger's Verizon card, communicated with Mr. Munger's computer, and Dr. Short was able to show you he could set up a virtual private network actually over the internet within five seconds by pushing one key.

After that seed had been planted, there was a few dried rocky years for these inventors. You heard they had a lot of difficulty getting their invention to grow and faced a lot of obstacles getting that done. But you heard that eventually the use of their invention became widespread, and that today anyone who needs to send important information confidentially and safely over the internet can shelter in the branches of the invention of Gif Munger and Bob Short.

Now, in this case, Judge Davis has already showed you the questions that he will ask you in writing the final chapter to this particular story. And what

I'd like to do over the next part of this argument is to go through those questions with you one by one.

Now you've already seen them, so you know that there are quite a few subparts to them that eventually you'll have to answer. But what I'd like to focus on for the next few minutes is just the four questions that he'll ask you.

These aren't the exact words that the judge uses but this is shorthand for the general subject that he's going to ask you in these first four questions.

First, does Microsoft infringe the patents? Second, is Microsoft's infringement willful? Third, are the patents invalid? And finally, how much is VirnetX entitled to as a reasonable royalty?

So let's start with the first of those questions. Does Microsoft infringe the patents.

Now, in bringing that evidence to you, we brought you Dr. Jones, Dr. Mark Jones from Virginia Tech University. You will remember that he testified on I think it was the second day of the trial and again this morning.

Dr. Jones, you heard, was allowed by Judge Davis to study the actual secret computer code that Microsoft uses in its products. You heard that he spent hundreds of hours comparing the claims of the patents to the Microsoft products and the Microsoft computer code.

Now two weeks ago at the opening statement I apologized and warned you that this testimony was going to be lengthy and it was going to be detailed. Turns out it was almost three hours long, and I explained to you then and as I explain to you again and apologize to you again now, the reason we had to do that is because we want you to be convinced that Microsoft uses each of these claims of both patents just as Dr. Jones went through in detail and explained to you step by step.

He didn't stop with a generalized conclusion, yeah, that claim is infringed, let's go on to the next one. Everyone of these checkmarks represents Dr. Jones taking the time to go through and show you step by step, yes, Microsoft does this, this, this, and this before he reached the conclusion and explained to you why Microsoft infringes that claim of the patent.

But what does Microsoft have to say about it? As I suggested to you in the opening statement, I think you have heard in this case that Microsoft will make any argument to you that they think will lead you off the path of requiring them to pay fair value for their use of this invention. If you don't buy the first one, they'll go on to the second one, and if the third and the fourth and fifth don't work, they have yet another argument in the hopes that eventually you'll find something that you think sticks and decide that Microsoft shouldn't have to pay fair value for their use of Dr. Short and Dr. Munger's -- or Mr. Munger's invention.

So what does Microsoft say at first? Well, of course they say we don't infringe. And the first reason that they give for claiming that they don't infringe is there's no virtual private network in our products. We don't have anonymity.

Well, we heard quite a bit of testimony and saw some evidence about that and here's an interesting piece of it.

This is a diagram that you were shown that was prepared by Dr. Johnson. You remember that he testified late last week. He was Microsoft's expert who was going to explain to you why they don't infringe. And he the testified to you that there's no anonymity because this sender of a message, Sue, her computer puts an address on the outside of the message that goes over the internet. That message goes over the internet addressed to, in this case, this Office Communication

Server which has its own address, and he told you this is not anonymous because this hacker can see those addresses as it travels across the internet. That's not anonymous.

But then remember when Mr. Caldwell was asking him some questions on cross-examination, and what he asked him was, well, Dr. Johnson, let's look at what you left out of your drawing. This is what he left out. The reason that you can send a communication safely across the internet to the Office Communication Server is there's nobody home on the Office Communication Server. That server doesn't have a keyboard, that server doesn't have a person sitting in it. That's sitting in a building somewhere that just does its job by its lonely self without any humans even being there.

What it does is to route this message down to the people who are actually intended to get it. And this address, Dr. Johnson admitted, is inside this envelope and is encrypted.

So what he told you is that, yeah, the hacker can see the information to send this envelope to the communication server, but he left out the part that told you that the actual identity of the recipient of the message is anonymous. Exactly what Judge Davis tells us the claims of the patent require.

We also talked about sender anonymity. Now you may remember here we were talking about a system called PeerNet. You remember that Dr. Johnson explained that you can have a whole group of computers and someone in the group may send a message out and a hacker may be able to see that the group sent a message but the hacker can't tell who it is within the group that sent the message. Is that anonymous?

Here's an excerpt from Plaintiff's Exhibit 2, the actual filing for the patent before the U.S. Trademark Office -- Patent & Trademark Office.

You remember there was testimony that this is an article about what anonymity in this context of internet communication means, and what it says is, A sender's anonymity is beyond suspicion though if the attacker can see evidence of a sent message, the sender appears no more likely to be the originator of that message than any other potential sender in the system. Exactly the situation that we talked about in Microsoft's PeerNet organization where yes, the attacker or the hacker may be able to see that somebody in the group sent a message, there's no way they can tell who it is in that group that sent the message. That is sender anonymity beyond suspicion.

Well, if you don't buy Microsoft's

argument that there's no anonymity, how about that there's no website. This invokes something that you've heard about from Judge Davis a couple of times called the Doctrine of Equivalents. And the simple meaning of that is there's two ways to show that there's infringement. One way is to show that Microsoft does exactly what's listed in the claim. The other way is to show that Microsoft does something that's substantially different, and that's just as good.

Here's what Judge Davis said. A claim limitation may be met in one of two ways; either literally or under the Doctrine of Equivalents.

A claim limitation is present in an accused product or method under the Doctrine of Equivalents if the differences between the claim limitation and a comparable element of the accused product or method are insubstantial.

Well, what about in this instance? This again may remind you of some of the testimony of Dr. Johnson.

Do you remember that when he was asking him some questions, Mr. Caldwell wrote on this board, all right, Dr. Johnson, you're talking about the differences between a website, that's what the claim says, and Office Communication Server, what Microsoft

02:59 does. And you're testifying to the jury that these two have nothing in common. That's what he said. And then he testified that they're completely different.

02:59 But then do you remember that Mr. Caldwell showed him a document from Microsoft saying they do have something in common, and then he showed him another document and another document and another document that all said the same thing until finally Dr. Johnson had to admit to you, well, this was wrong. I was wrong to say that they have nothing in common.

03:00 Completely different? Same story.

03:00 Mr. Caldwell showed him first one document, then another document, then another document to say they're basically the same until Dr. Johnson had to tell you, well, I was wrong about that too. When I testified to you that they were completely different, they really weren't.

03:00 Well, if you won't buy Microsoft's argument that they don't infringe because of the website, how about the gatekeeper computer? Well, really the only testimony you heard in this case has been from Dr. Jones and he testified to you that yes, the gatekeeper computer can be met by the Microsoft software, the functionality of that in the Office Communications Server product.

Okay. If you don't buy that, how about secure computer network address. This again is Dr. Johnson. He showed you this picture and he said, well, see this part over here, this is out of the patent. And you see what it shows is that what the patent is talking about is to have this secure address, you have the SCOM, that's the secure communication, and the COM, that's the regular unsecured, and you see that they each have their own independent connection to the internet.

Well, that's not what we do at Microsoft. At Microsoft, if you're in a group meeting using our software, you can communicate securely with other members of the group, but at the same time, over the same connection, you can communicate just out in the regular unsecured internet, so we don't -- we don't have this different connection.

But then Mr. Caldwell said to him, yeah, but what about this part of the picture. What this part shows is the secured communication and the unsecured communication both communicating with the internet through the same communication channel. Exactly what Dr. Johnson told you Microsoft does.

Ladies and gentlemen [sic] of the jury, I think you'll find that every argument about infringement

Microsoft has made to you is nothing more than an attempt to lead you off the path of requiring Microsoft to pay fair value for using this invention.

If after considering all of the evidence in your deliberation, if you believe in response to question 1 that VirnetX has proved by a preponderance of the evidence that Microsoft infringes, then you should answer yes as to the '135 patent and answer yes as to the '180 patent.

The second question that Judge Davis will ask you to consider is is Microsoft's infringement willful. The first thing that we, VirnetX, are required to show you in order for you to find that infringement willful is that Microsoft knew of the patent. Well, there's not any question about that. Here's a communication that Microsoft got in 2003 from the U.S. Patent Office specifically telling Microsoft that its patent was being rejected because of the Munger '135 patent, the patent we're here, one of them, talking about.

And then we've seen this document several times. In May of 2006, SAIC who owned the patent at the time sent this letter to Mr. Gupta who sent it to Mr. Smith in the Microsoft legal department who sent to it Mr. Marshall Phelps who was the head patent lawyer for Microsoft.

In this letter that you've seen a number of times, SAIC suggested we'd like to contact you to discuss the possibility of offering a license to the patent. It enclosed a copy of the patent; it named the Microsoft products that we're talking about here today.

Now several letters went back and forth between the parties, but the fact of the matter is that Microsoft has never agreed to pay fair value for this patent.

And after getting this letter, what steps have they told you about that they took to avoid infringing after they've been told you need to take a look at this?

Mr. Pall testified did Microsoft, after receiving this letter, take any steps to avoid infringing the '135 patent?

He answers: I do not know of taking any steps. I know there was follow-up to the letter, but I do not know of any steps we would take on infringing the letter.

And I said now you said it. And he corrects himself I -- I said it on infringing the patents.

Mr. Pall who was a vice-president in that very business division, he doesn't know of any steps they took. And why is that? I'll suggest to you it's because of the next deposition testimony you heard, not from a man like Mr. Pall, very senior in Microsoft, but a deposition you heard from one of the little people, the man who spends his day writing software all day long. That's Mr. Ryan Kim.

He was deposed, a Microsoft design engineer, and he said, We were actually expressly told not to look at patents.

Question: Who told you not to look at patents during the development of Meeting Space?

Answer: It's a pretty well-known practice inside Microsoft for developers.

Ladies of the Jury, were you shocked when you heard that? Were you shocked that a company of the stature of Microsoft would tell its employees not to even look at the patents of others.

What does Microsoft have to say about its infringement being willful or not? Who have they brought to court to explain to you, well, here's the reasons why we really thought we were infringing, here's the reasons back when we got that letter in 2006, you know, we looked at this and we just decided the patent must not be valid? Nobody. Nobody has come to explain

03:06 to you any reason whatsoever that Microsoft can offer why it chose, after getting that letter or getting that notice from the Patent Office how it formed any kind of reasonable belief that it was not infringing a valid patent.

03:06 If you believe that Microsoft's infringement was willful, then when the time comes to answer the jury questions as to the '135, you should answer yes, and as to the '180, you should answer yes.

03:07 So that brings us to the third question Judge Davis will ask you to consider: Are the patents invalid?

03:07 Now here the situation is a little different because as Judge Davis has told you several times, it's Microsoft's responsibility to show you that the patent is invalid and to do so by clear and convincing evidence. Now why is that? Judge Davis has explained it to us.

03:07 On the very first day of the trial, he read you some instructions and here's what he said. He said that the granting of a patent by the United States Patent & Trademark Office, however, carries with it the presumption that the patent is valid.

03:07 However, the granting of a patent by the Patent & Trademark Office carries with it the presumption that the patent is valid. This is another place in the same instruction he said that sentence. The presumption of patent validity imposes the burden on Microsoft to prove invalidity by the clear and convincing evidence standard.

In other words, what you've heard is that because the United States Patent Office spent more than two years examining the first patent and more than seven years studying and examining the '180 patent, there is a presumption that they did their job properly.

Judge Davis told you just today an issued patent is accorded a presumption of validity based on the presumption that the United States Patent & Trademark Office acted correctly in issue a patent.

So the question on this issue No. 3, invalidity, really is what has Microsoft done and shown you to convince you by clear and convincing evidence that Microsoft should not be required to pay fair value for their use of this invention.

Well, they'll tell you, of course, that the patent is invalid, and the first reason they'll give you is the Windows NT system using AutoDial, that did it first. That did it back in 1996, and indeed we'll bring you in a demonstration and show you.

Well, let's talk about that demonstration you saw. The three computers, the three beige computers over here and the one beige computer here and under the table.

The first thing we noticed on cross-examination was that sticker we've heard about that said Windows 2000 Professional on it. Now you've heard testimony that that's just a sticker on the outside of the computer. It doesn't necessarily tell you anything about the date of the software that's inside the computer, but it was the first red flag that maybe things weren't really like Microsoft was telling you they are.

So the next thing I did was to ask Mr. Pall to go into the computer and to open up some critical software called the BIOS, the basic input/output system. You remember that he testified to you that without the BIOS, without that software, the computer would not work. Without that software the system that you saw demonstrated by Mr. Pall could not be built.

And do you remember when I asked him to push the right buttons and pull up the right information, he had to admit to you that that software on the computer that he told you was from 1996 was dated July 2000. Six months after the patent was filed.

But we didn't stop there. Mr. Wicker testified about this feature in that demonstration called AutoDial and here's what he told you. He says that AutoDial only reconnects a user. Do you agree with that?
His answer: Reconnect -- yes. I would say it reconnects in the sense that you have to have it connected once before at some point in time.

Question: And its only function is to reconnect to a user, right?

Yes, that's correct.

Question: We don't know how that VPN was initiated for the first time, do we?

Answer: No.

When Mr. Pall sat here and told you that with one click he was connecting to a VPN, remember, the way Microsoft supposedly did it in 1996, what he didn't tell you was, that was a reconnection that he or Microsoft's lawyers had to do it for the first time a different way.

And my question, ladies of the jury is, why didn't they show you what they had to do to make that first connection? And I'll suggest to you, because it would look a lot like what Dr. Short spent about 20 long minutes explaining to you how difficult it was to do it -- not in the reconnection, but the first time.

But there's more.

You'll remember that one of the claims of the '135 patent says that part of the invention is that the DNS request, the domain name service request that gets typed in and you hit the one click, that has to determine whether the user is looking for a secure site or just a regular site.

That determining step was something Mr. Pall was asked about. Isn't it true, don't you agree, Mr. Pall, that the system you're demonstrating is not determining whether the VPN DNS request transmitted is requesting access to a secure website?

And by that time he had to admit, the system is not determining that specifically, sir. The system from 1996, that supposedly means that Microsoft did it before these inventors, it didn't do what they invented. And Mr. Pall admitted it right here.

And finally on this subject of the Microsoft NT with AutoDial, this is how Mr. Wicker did his study to tell you about the source code, the computer code for that AutoDial and NT product.

You remember he told you that he studied that code and he says here that the key source code relating to Microsoft Windows NT 4 is what he studied, that's the product we're talking about from 1996, NT 4.

And now down here he lists one of the pieces of source code he looked at, sure enough, Windows 4. That's the NT 4 product.

But you remember when Mr. McLeroy asked him questions on cross-examination and he said flip about halfway through that big fat stack of computer code, and what we found was he slipped in Windows NT 5. Different software.

When Mr. Wicker -- Dr. Wicker testified to you that NT 4 did it all, they did the invention before Mr. Munger and Mr. Short, he didn't tell you that he mixed and matched that software and later software in order to be able to come to that conclusion.

Well, if you won't buy, says Microsoft, that Windows NT AutoDial makes the patents invalid, how about DVPN? Well, DVPN was a product that DARPA, this government agency, paid to have developed. It was -- something was demonstrated exactly once in March of 1998. But the question is what really got demonstrated? What clear and convincing evidence have you seen and heard to tell you what happened at that demonstration?

Well, you heard from one man who was there, Mr. Sami Saydjari. He's the man that Microsoft was paying $475 an hour. He was asked, Do you have any recollection of whether the DVPN system used in the --

used the DNS request to trigger a VPN? Remember that? That's the basis of the invention you use the DNS request to trigger the VPN.

He said, I don't have a specific recollection, but given my recollection of the coalition manager, the CM being centrally involved, I would doubt that they would use the DNS call to trigger. He doubts that that even worked that away.

So what else has done -- has Microsoft done to bring you clear and convincing evidence? Well, they and VirnetX told you about one man who wrote the computer code for DVPN and who went to that demonstration and actually demonstrated it. He's the man who knows what was in it. He's the man who knows what parts of it were actually demonstrated to the public.

His name is Domenic Turchi. He was from Maryland we knew from some documents. So you heard that Mr. McLeroy, when he entered his name the search request, found Domenic Turchi, Jr., in Maryland, his phone number, his address. And if you click on this link right here, it'll even give you a map to his house. But Microsoft didn't bring Mr. Turchi here to testify to you.

Remember, it's Microsoft, with Microsoft's resources, who bears the burden of trying to convince you that somebody else did this first and to convince you by clear and convincing evidence.

I would respectfully suggest to you that on this DVPN, the combination of Mr. Saydjari saying I don't really remember how it triggered, and Microsoft bringing no one else who can tell you what happened in that demonstration is a failure of their obligation to prove that to you.

Well, if you haven't bought Windows NT with AutoDial and you haven't bought DVPN, they've got more. How about Aventail. Maybe you'll believe that that should make the patents invalid.

Dr. Jones, though, you'll remember, just this morning testified that Aventail is a point-to-point technology. One computer to one computer, not a network-to-network technology.

And Mr. Pall testified, You agree, therefore, that a VPN is more than just a point-to-point connection?

And then here was some evidence on another issue about Aventail. Secure domain names. The patent required that there be secure domain names. Aventail doesn't use them. Didn't use the standard domain names.

Well, Dr. Wicker was asked about this, and

I have to say I believe and I'm going to suggest to you that in an effort to try and salvage his argument that Aventail renders the patents invalid, he said, well, yeah, Aventail uses standard domain names but they can overlap with secure domain names so they may be the same thing.

But Dr. Johnson for Microsoft was asked the same question, and he said no, they can't. They don't overlap. Microsoft's Dr. Wicker says yes, Microsoft's. Dr. Johnson says no.

Now, ladies of the jury, you may be asking yourself, well, how are we supposed to know? I mean -- I mean, these two men are experts. A week ago some of us had never heard of domain names and standard and secure. How are we supposed to resolve one -- one says yes and one says no?

I will suggest to you, ladies of the jury, Judge Davis will tell you how. He's already told you there's a presumption of that the valid patent. And unless Microsoft proves different to you by clear and convincing evidence, you should find the patent is not invalid.

And I will finally suggest to you that this kind of contradiction between Microsoft's own experts is nothing like clear or convincing evidence.

If, after considering the evidence, you find that Microsoft has failed to prove to you that the patents are invalid by clear and convincing evidence, then on column 3, under Invalidity, you should answer no, the patents are not invalid as to the 135; and no, the patents are not invalid as to the 180.

Now that brings us to the last of the four questions that Judge Davis is going to ask you to consider. How much is VirnetX entitled to as a reasonable royalty?

This is the summary of the work that Mr. Reed did as he testified to you at some length about how he arrived at a total reasonable royalty of $242 million.

Now I'll go through this a little more in a minute to point out some specific matters to you that you might want to keep in mind. But let's talk about what Microsoft says to you: No, you -- there should be very little royalty for this invention.

Dr. Ugone, who you heard testify for Microsoft this morning, says IT shouldn't be anymore than $15 million. Well, why do they say that that's so?

Well, first of all, they say what about all the failures. Remember the businesses that weren't interested in this invention and all the work that

Mr. Munger did, all those failures show this isn't worth anything.

You know, when I heard that, I couldn't help but remember back to an earlier time in my life, and I'll take just a minute to share it with you.

It was when I was in junior high. I was in the seventh grade. You remember I told you I grew up in Arlington and back then there were no big stadiums, no Six Flags, and the junior high that I went to was so small that they had one football team for the seventh and eighth graders.

And I'm new to junior high, so I decided to go out for the football team that year. And I was a lot smaller then than I am now and a lot skinnier, and I learned that I was just about the smallest kid who was going out for football.

Well, after a couple of days of that, I decided I was going to quit. So, I went home and my grandfather was there, and this was the kind of thing that I'd usually share with him. So I told him, I'm -- I'm not going out for football. Football is boring. The coaches are stupid. I don't want to do it.

Well, as was his way, he didn't argue with me, he didn't give me any advice, he just sat there and after minute, he said to me son, a little man can beat a

03:23 big man if the little man's tough and keeps on comin'. Well, I took that advice to heart, and I was on the football team that year.

03:23 But I have to say that that reminded me of Mr. Munger and Dr. Short.

03:23 After they conceived of this invention, they went out and tried to raise money from venture capitalists. Mr. Munger talked on the road day after day to more than 30 investors and they all said no, but he kept on comin'.

03:24 Then he went off to some companies like Amazon, like J.P. Morgan, like others you've heard about in the proposal. Why don't we do this, why don't you invest money and we'll show you how to do it. They said no, we can do things ourselves. We're -- we don't -- we're not interested. He kept on comin'.

03:24 He went to government agencies that you heard about, Homeland Security, others. Couldn't get them interested at that time. He kept on comin'. His own company decided they could no longer continue to fund the development. He got a license from the company called SafeNet, but they were required to spend a lot of money to develop the product and they decided they wouldn't do it. He kept on comin'.

03:24 By this time five years had gone by, and

03:25 Mr. Munger, pretty much by accident, discovers that Microsoft is already using his invention. And I'll suggest to you that at that point, he, Dr. Short, and others basically had two choices. One choice was they could contact Microsoft and propose a reasonable arrangement where Microsoft would pay them fair value for using the invention. Well, they did that.

03:25 The reason we're here today is Microsoft refused to pay fair value for the invention. The only other choice they had was to file a lawsuit against the largest software company in the world. And these two men have battled through three long years of litigation until they finally get to come to this day when they can present their case to eight jurors in Tyler, Texas.

03:26 Ladies and Gentlemen [sic], Microsoft may call these two men failures. I call them tough.

03:26 Now, what does Microsoft have to say about the value of this invention that supposedly no one wanted? Well, you saw this document.

03:26 Microsoft says, We believe unified communications which is -- depends on these inventions will transform business in the coming decade in the same way e-mail changed the business landscape of the 1990s. Here's a document from 2001 saying that, RTC which you've heard uses the invention, is one of the top five reasons to buy Windows XP, Microsoft's new flagship operating system product.

In 2007, Microsoft said, For Windows peer-to-peer is a natural destiny. With market leading install base of clients, Windows can create the largest P2P systems. Over the past several years, we've been working to realize that P2P destiny. A destiny that depends on their use of these inventions.

In August of 2006, they said that Meeting Space -- you remember you heard that product described and you heard how it uses the invention -- is being positioned by marketing as one of the top enterprise features for Vista client.

Ladies of the jury, Microsoft thought this invention was very important.

Here's the back of the box of Windows Vista Operating System. You may remember that this was the hot new Microsoft product from about 18 months ago. On the back of the box this home edition, it lists seven reasons why you, the person looking at this box and trying to make a decision, should decide to buy this product. And one of those seven is you can collaborate and share documents with Windows Meeting Space, a feature that depends on this invention.

Well, the invention, I'd suggest to you, hasn't been a failure at all. Microsoft has made a great success of it and has made an enormous amount of money from using it.

Well, what else will Microsoft tell you about why you should award only a little royalty. Well, they'll say the damages haven't been apportioned. There's lots of features in this complex software and you haven't accounted for all of those.

Well, here's the slide you saw from Mr. Reed setting forth in a lot of detail how he apportioned the money that Microsoft made from selling these products, 48 billion, down to 33 billion for some features in the software that he could say definitely had nothing to do with the invention, down to 30 billion from Microsoft's market size and contribution.

Then he arrived at the opinion that not 20 percent like the SafeNet license but only 1 percent per patent would be a fair royalty.

But he didn't stop there. He said that because this tree of invention was still growing back in 2003, it would really be fair only to start off at one-third of 1 percent growing to two-thirds of one percent per patent in 2008. What he's telling you then is he has apportioned down to what this invention is worth down to one-third of a penny per patent for the money that Microsoft has made from the invention.

He explained to you here that if he hadn't done that, if he hadn't made that apportionment, the number he would have told you was reasonable was $704 million instead of the number he told you was reasonable, 242.

Well, finally Microsoft will tell you, okay, if you don't buy failure and you don't buy not a portion, how about lump sum. Maybe you'll believe that the parties would only have agreed to a lump sum. But you see, the thing about that is, what Mr. Reed explained to you is if Mr. Munger and Microsoft had set down at the table in 2003 and Microsoft had said, okay, we're not going to pay you as we go, we're just going to pay you one sum today, not just for today and not just from tomorrow, but all the way to the end of the life of this patent, that's what it would have taken to do that deal. And Mr. Reed explained to you that number would have been something like $942 million.

Now, he didn't suggest to you that that's the amount you should award as a reasonable royalty. He suggests to you that because it would take so much money to compensate VirnetX and the inventors for the entire life of the patent, that Microsoft would have agreed and Mr. Munger would have agreed to a pay-as-you-go running royalty deal.

Now, for those of you who -- who are accustomed to dealing with numbers on the page, here's how Mr. Reed arrived at the separate damages figure. First of all, on this top line, he calculated the '135 damages, that's right here, for Windows XP Vista, and the '135 for Microsoft LCS/OCS. So the sum of these two numbers represents the total damages for the '135 patent. That's $158,700,000. I'll show you that number again in a second.

For the '108 patent, that's not implicated by these Microsoft Products, so the '180 patent is $83,600,000.

Ladies of the jury, if you refuse to be led off the path of fair value by Microsoft's many arguments, and if you believe the testimony of Mr. Reed and others as to the amount that is a fair and reasonable royalty for the use of these patents, then the damages for the '135 patent would be $158,700,000, and for the '180 patent $83,600,000?

THE COURT: You have 10 minutes left, Mr. Cawley.

MR. CAWLEY: Thank you, Your Honor.

Ladies and gentlemen [sic] of the jury, Judge Davis has told me that I have 10 minutes left.

And the rules of these lawsuits that Judge Davis runs herd over so well allow me to save those 10 minutes so that I can come back and talk to you again just for those 10 minutes at the very end of this argument.

I'll tell that when I do that, I'm going to want to go back through these four questions that Judge Davis is going to ask you so that we can review one last time the evidence that you may find is important in making your decision. Thank you.

THE COURT: All right. Counsel for Microsoft.

MR. POWERS: Thank you, Your Honor.

MR. SAYLES: May I move these and give some room to Mr. Powers?

THE COURT: Yes, you may.

MR. POWERS: May I proceed, Your Honor?

THE COURT: Yes, you may.

MR. POWERS: Good afternoon.

This is a lawsuit that never should have been brought. The reason is the facts don't support it. Judge Davis told you at the very beginning of the case and he also told you again now that what should guide your decision in the case are the facts, the facts that are relevant to the issues he's asked you to decide, not emotion, not prejudice, not anything like that, but the facts relevant to the issues he's asked you to decide. And those facts suggest this lawsuit should never have been brought.

As I sat listening to the witnesses testify, it occurred to me that there were three things that were happening, and those three things I wanted to summarize for you because they were helpful to me in organizing my thoughts about the case.

The first is that this case, unlike many others, is really about the difference between people's hopes and the reality. There's no doubt that Mr. Munger and Dr. Short hoped that they had solved the problem of the internet.

That's what they testified they thought they did. The reality is quite different. They're asking you to pay them as if they had solved that problem.

A second thought that occurred to me when I was listening to particularly the cross-examination of Microsoft witnesses was the difference between words and facts. And I'm going to show you some examples of that as well.

There's a lot of words that have been thrown around this courtroom, but the facts that are relevant to your decision I'm going to summarize in a

03:36 way that we think is relevant and ask you to decide based on those.

03:36 And last but not least is the question of distractions versus the real issues. You'll recall that Mr. Cawley, at the very beginning of his opening statement, put a picture of a sign post up with the distractions. I'm going to come back to and put it up on the screen and see how distracting they were.

03:36 Now let's talk about hope versus reality. This is from the opening statement by counsel for VirnetX, and he said they solved the problem of secure communications over the internet.

03:36 That was the hope. They thought they might have done that, but they didn't. How do we know they didn't? Because that is a real problem. It always has been and always will be.

03:37 And if you truly, truly solve that problem once and for all better than everybody else that did, that would be worth money. But we know that, in fact, everybody who looked at their technology said this doesn't do that. That may be your hope, but it's not the reality.

03:37 The CIA, who looked at their own invention, got the source code and said: Nope, we're not funding it anymore. Why? Because the product has

03:37 not lived up to expectations. That was the CIA's or In-Q-Tel's own analysis after looking at the source code.

03:37 High hopes before they looked at the product; rejection afterwards. And they actually use some pretty harsh words. The President -- the CEO of that group called it: The living dead category. And for that living dead, the product not living up to its expectations, they want $242. The CIA wouldn't even give them two.

03:38 Their own company, SAIC, they knew exactly what this was worth. They say: We're not going to pull -- we're going to pull the plug. We're not going to fund you at all.

03:38 If it were really worth $242 million, don't you think they would have invested the seven that Mr. Munger asked for? They knew what it was worth. They pulled the plug.

03:38 Venture capitalists, they were in the business of making money funding people who have great ideas. They talked to 32 of them. All 32 said no.

03:38 They talked to the CIA, the FBI, Homeland Security, each of which had a free license to these patents, free, and they still said no.

03:38 They talked to companies who are

interested in internet security, desperately interested in it. If this product with their technology really had any value, somebody, somebody would have funded it. Somebody would have bought it. It didn't. That's the reality.

The hope was they had done something great. The reality was very, very different.

SafeNet was the very last possibility. Remember that? They had gone through 2001 and SafeNet finally says: Well, we'll take a license, but we want to look at the source code first and really see if this is worth it.

When they got the source code and looked at it, they said: Well, it doesn't really accomplish any simplicity. It just moves that complexity around. SafeNet terminates the license, pays nothing. The reality is what they're asking you to give them $242 million for.

Everybody who has looked at their technology closely, who had the technical expertise to evaluate it, who had the economic motivation to invest in it or buy it because it would be worth a lot of money if it really worked, all of those people said no. That's the reality.

Now, what excuses have we heard for that?

Well, the first was: Well, September 11th changed everything. Nobody was going to invest in this type of technology anymore.

Well, it turns out it was the opposite. In fact, in a memo that Dr. Short had talked about, he admitted that, in fact, September 11th increased the demand. As an article they were circulating around internally said: They're jamming the pedal to the metal on spending for information security. It didn't slow it down; it sped it up.

So that excuse didn't work. What was the next excuse? Well, we're in a recession. Remember you heard that from both Mr. Short and Mr. Munger. But that recession didn't stop Aventail from getting funded. They were funded in October of 2001, not only after 9/11, but right in the middle of the very recession these guys were talking about.

And they were not just funded by anybody. They got $7 million from Mr. Munger and Dr. Short's employer, SAIC.

So the best analysis of reality that you can have is SAIC knew the facts back in 2001. They knew which technology was valuable. They knew which technology was first.

Mr. Munger asked $7 million. SAIC said

no, even though it was their own project that they had already invested something in. They took that 7 million and gave to it Aventail, which was first and worked.

So it wasn't the recession. It wasn't 9/11. So what's the next excuse? Well, the next question that's been given is: Well, we can't compete if Microsoft is out there. You heard that from almost everybody.

Well, the problem with that is timing. As Ronald Reagan once said, facts is stubborn things, and the timing just doesn't work. They ran out of money in October of 2001. The products they're complaining about competing with them didn't happen until 2003, two years later. Facts are stubborn things.

Now, we're not saying, as Counsel suggested, that these men are failures. No. They succeeded with Global Hawk. They succeeded with many things in their lives. We're saying this technology failed.

And that's okay. As I said in opening statement, there's no shame in having a project that you worked on fail. It happens to companies all over the place. It happens at Microsoft. We've had some clunkers over the years as well.

But what you're supposed to do then, as I said in opening statement, is pick yourself back up and go make something people want. Go make something that works. That's what Mr. Pall did.

Mr. Munger and Dr. Short, instead of being in this courtroom, should be back working on something that works that people want. Then they'll get paid. Then they'll get money, because that's the way the system is supposed to work.

Words versus facts. Well, you saw them point to this word anonymous, and say, well, obviously, it's anonymous. No, no. That's not a fact; that's a word.

The fact, according to their own expert, is that that hacker, using our products, would know which computer is talking to which other computer. Not anonymous at all. Words versus facts.

Another word, they say: Well, Microsoft changed its website from serverless DNS. Is serverless DNS a requirement of the claims? No. Secure domain name service is a requirement. And we're not arguing about that. That's just words. Not a fact that's relevant.

Rejected. You heard Mr. Cawley talk about this: That Microsoft's patent was rejected based on Mr. Munger's patent in the Patent Office. Well, it turns out later it was actually allowed. The Patent Office gave Microsoft the very patent that they were talking about.

The next thing I want to talk is distractions versus real issues. And this is actually a very central theme of this case. Mr. Cawley set this theme in his very initial opening statement. And he showed you this slide, and he said: These are Microsoft's distractions.

Well, no infringement, that's the very first question you're being asked to decide on the verdict form. That's a distraction? That's what they have to prove.

Not willful. That's the second on your verdict form. That's what they have to prove.

Third supposed distraction invalidity? Well, that's exactly the next issue on your verdict form. That's not a distraction. Those issues that he accused us of raising are the issues that they have to prove and that you have to decide. Those aren't distractions.

Fourth issue, that the patents aren't valuable. That goes directly to the fourth question, damages. How much is it worth?

So these supposed distractions for

Microsoft are exactly the four issues you have to decide. But there are distractions in this case, and I want to talk about a few of them.

The first is exactly the one that Mr. Cawley just referenced in his closing argument. Remember, Dr. Short, who got up in front of you and marked up all over the board, he was saying that he went out and investigated the ways that you could do remote access.

Remember our remote user? And he used this slide over here. Let's talk about it. He said: I looked at how people used remote users to contact and I found out that they're very complicated. And then he spent, as Mr. Cawley said, 20 more minutes marking up all of that.

Now, you would expect that if he spent that time, that he was talking about a product that was designed for exactly this situation, for a remote user.

This is his markup that he did extensively. It turns out, when you look at the product that he was marking up, it says that it's not supported for client remote access, VPN. That's not what it's for.

So he was criticizing a product for not being good for a purpose for which it was not designed, and he knew it.

Now, there's another product that is designed for remote access that he could have looked at but didn't, and that was exactly the product that Mr. Pall described and demonstrated to you, which was PPTP.

It had come out four years earlier, and it's specifically designed for remote access and remote users. Did he mark up the user's manual for PPTP in front of you? No. He chose something called IP SEC that wasn't designed for it at all. That is a distraction.

The fact is, we weren't arguing that IP SEC was a relevant piece of prior art here. We weren't arguing that that's what you should consider, the old IP SEC. We were saying look at PPTP.

He didn't choose to mark that up. Why? Well, because it's easy. PPTP is easy of use -- easy to use, the easiest way to do it. He demonstrated with one click. That's why he didn't demonstrate that or criticize it, because he couldn't. That's why what he did do was an attempt to distract from the facts that are relevant to your decision.

Now, you've heard Mr. Cawley say: Well, PPTP has a user's manual that's 25 pages long. So is

03:47 theirs. That's the difference that Mr. Pall pointed out between the mechanic and the driver.

03:47 The mechanic has to look at a thick user's manual for any of this product. The issue is, how easy it is for the driver. Mr. Pall showed that with one click, 1996, four years before their invention.

03:47 The VPN connection can be set up and activated from one easy AutoDial phone book entry. Click on that entry, and you're done. They didn't criticize that. They didn't demonstrate that.

03:48 Other distractions that you've heard a lot about from the VirnetX side of this case, scud missiles, Global Hawk, FBI antiterrorism.

03:48 We applaud whatever work they've done in this area. They're not relevant to this case. They didn't invent anything relevant to this case with all of that. Yet they've spent a lot of their precious, scarce time talking about all of that.

03:48 The Windows 2000 sticker. Mr. Cawley still talked about it in closing argument. Remember he made Mr. Pall get down on his hands and knees. He made Ms. Weiswasser move out so that we could all huddle around and look at this 2000 sticker.

03:48 And then you heard their expert, their technical expert, Dr. Jones, say, well, that sticker didn't mean anything. Why? Because you can look right on the monitor and see that the actual software running was 1996. That sticker was an older stick in an old box.

Dr. Jones admitted that in front of you today. And he knew it, and their lawyer knew it, but they chose to make everybody go down on the ground and look at a sticker that meant nothing. That's a distraction.

The facts are it was 1996 software. He talked about BIOS. Dr. Wicker explained how that doesn't affect 1996 software at all. The software was 1996. Dr. Wicker said it. Dr. Jones said it. The lawyers' arguments don't change those facts.

The next distraction was consulting rates. Mr. Saydjari. Their suggestion, I guess, is that he's the only person who should be here for free, even though he doesn't have a dog in this fight.

Mr. Munger is getting paid. Dr. Short is getting paid. The lawyers are getting paid, and the other experts are getting paid. Saydjari should come here from Wisconsin for free, even though it takes him away from his business? That's a distraction.

What is the evidence? Well, the evidence is, he was there at the demonstration, and it was wildly successful.

Now, the next distraction, Domenic Turchi. Saw it again in closing arguments. Why didn't Microsoft call him? Why didn't -- why didn't they call him? We called three people to testify about this product, VPN: Mr. Saydjari, Mr. Sterne, and Mr. Kindred.

Mr. Sterne led that project; Mr. Kindred led that project after Mr. Turchi; and Mr. Saydjari was the one who was funding that project. They are the right people. If they wanted Mr. Turchi here, they could have brought him here.

Now, those are the distractions. There's a real question, though, about missing witnesses.

Where is Kendall Larsen? Kendall Larsen is the CEO, founder, President, Chairman of the Board, largest single stockholder of VirnetX. He's the man who stands to gain the most from this, and he didn't even bother to show up.

Now, there's a reason for that, because his testimony tells you the reason for that. You remember all this testimony about the letter that was sent from SAIC in May of 2006. VirnetX counsel showed it to you again in closing argument.

It asserted that this RFC 3263 is the reason Microsoft infringes. Well, Mr. Larsen said:

Yeah. That was a mistake. They didn't want Mr. Larsen here to talk -- to have to answer to that.

You know, another very important about Mr. Larsen is that you'll remember in 2006, he asked that company called Magenic, Magenic, M-A-G-E-N-I-C, to take the two specific products that are accused here of infringing, Office Communicator and Live Communications Server, and he said: Please add to them and make them work using our patents. Add our patented technologies to those products.

And he had raised a little bit of money by that point, and he spent it all trying to do that. But here VirnetX says those products already infringe. Why in the world would VirnetX have spent the only money it had raised trying to make those products work, according to their patents, if they already did?

Mr. Larsen could have answered that. Mr. Munger first disagreed with me, said: Well, I don't think he was trying to modify those products to add VirnetX's patented technology. He disagreed. And then he said: Well, that's a real surprise once I showed him the documentation.

I guess Mr. Kendall Larsen would have to answer that because he was there, and I wasn't. So what did Mr. Larsen say?

QUESTION: The objectives were to modify Microsoft's products to utilize patents -- VirnetX's patented technology in those products.

ANSWER: Correct.

Yet those are the very same products that VirnetX is standing in front of you here and saying already use them.

03:52

Now, why in the world would Mr. Larsen spend the only money he had raised trying to convert Microsoft's products into one that used the patents if they already do. Well, Mr. Larsen chose not to come here to have to answer that.

But it goes beyond that. You'll recall that he submitted a sworn affidavit about when these patents were invented, September 23rd, 1999. I showed that to Mr. Munger. He said: Oops, that sworn statement is not true. It was false.

They chose not to bring him here for that reason, too.

The second person that's not here that should be, particularly when you're asking for $272 is Dr. Victor Larson. And he's not here for a reason. He's one of the co-inventors, so they certainly could have brought him. And why didn't they bring him?

Well, he said the patents provide -- don't provide any amount of protection. It's real hard to see from here, but don't provide any amount of protection for something which is SIP secure. But that's exactly what they're accusing here.

So Victor Larson, one of the inventors, he knew there was no infringement. He knew it, and that's why they didn't bring him to testify to you.

Mr. Munger says the products they say infringe here use SIP plus TLS. Mr. Munger agrees. That's what they're here in front of you saying infringes.

So what does Dr. Larson say? This was in the deposition testimony that we played today. He had a strong feeling that the patent provided no protection against secure SIP using TLS. And he hadn't changed his mind even after studying the patent and all of that information.

That's why those two key people aren't here. Both of them knew there was no infringement, and they said it, and their actions confirmed it. So they bring other people here to ask for $242 million.

So what excuse did they give? Dr. Short says: Well, we have pretty limited time. Well, they could have spent a little less time talking about Global Hawk and scud missiles just to bring the two key people who could have answered the questions that this Court has asked you to answer, particularly when they're asking for $242 million.

Why didn't VirnetX call any SAIC witnesses? The letter they keep relying upon is from Pamela Bumann from SAIC. And they say: Well, she says she never even got that September 2006 letter from us.

Hmmm, maybe that's why. Because Mr. Larsen said, yeah, he got it, and it wasn't even addressed to him. So where did he get it from, if not her?

So probably that's why they didn't bring her, but she's the one who sent the letter who could have testified about why she didn't send Microsoft the information it asked for when it said: Put up. Show us the reason we really infringe, according to you. They didn't.

And why there was no meeting when Microsoft said, yes, let's have a meeting; why, instead of having a meeting, why, instead of giving us the information we asked for, why all they did was transfer the patent to VirnetX so they could sue us. That tells you what kind of case this is, what the case is about. Not distractions.

First, do we use the VirnetX's patents?

That's infringement.

Second, was VirnetX first? That's anticipation.

Third, are those claimed inventions obvious?

Let's talk about infringement first. Judge Davis' construction says, if they're missing only one of those limitations of the claims, there's no infringement.

On the '135 patent, they're missing two: The VPN and the website. Those aren't distractions. Those are things they have to prove. Those aren't distractions off the path. That's part of the requirements for their claim that Judge Davis has laid out in the instructions.

So let's talk about VPN first. The issue is anonymity, of course. You've heard a lot about that. Judge Davis' construction. Dr. Jones admitted that the order requires anonymity, so the question is, does it provide anonymity?

The patent tells you what that means. You want to prevent an eavesdropper from discovering that Terminal 100 -- that's a computer -- is talking to Terminal 110, another computer.

So let's look at the accused product and see if that's true. Can an eavesdropper determine that one computer is talking to a second computer?

Dr. Jones says that's exactly what that means. Anonymity says you can't determine the identity of the computers that are talking with each other. They agree.

Now, this is what they're accusing. Now, Office Communicator talking to OCS, those two computers have one address that defines them and one only. That's like their name. And that address is visible plainly over the internet. There's nothing hidden as to that address. That address identifies those computers, and it can be seen.

And Dr. Jones admitted that. He admitted that by his own Wireshark data. This is his slide that he showed you. That address from that sender is visible. That address from that recipient is visible.

And he admits that our eavesdropper would know that this computer is in communication with that computer. That's about Office Communicator. He admits that that is true. But that is exactly what the patents say can't be true for infringement.

In the '135, anonymity is preventing an eavesdropper from knowing that one computer is in communication with another. But that's exactly what he admitted is true in our case. Their own expert, who they brought to try to prove infringement, admitted no anonymity.

And on the question of whether it's a VPN, we showed you lots of marketing material that said one of the benefits of Office Communicator is you don't need a VPN. We said over and over again that it doesn't require a VPN. That's why it's -- one of the reasons it's better.

Remember, Dr. Jones said: Well, I think that might be saying you don't need another VPN. And then he admitted that's not what any of the facts said, and even more so, Office Communicator is beneficial when VPN connections are not possible.

So not only is it not a VPN, as required for the claims; the advantage of it is you can use when VPNs aren't even possible.

So what does VirnetX have to say? They have a lot of arguments here.

The first one is: Well, there's always an IP address. You can't hide that. That's from Dr. Jones.

And then on cross-examination, he admitted: Well, there are different ways you can hide that IP address. It's just that Microsoft doesn't do it. There are ways you can hide the IP address so that you don't know which computer is talking to which other computer.

And the first one was from the book he used with his own class at the University of Tennessee. It says: The identify of the original source and destination are hidden in a VPN, and only addresses of the outer routers are visible.

So that's one way of hiding those actual true addresses of the sender and receiver. You use what's called -- what they're calling a tunnel.

Dr. Short's own demonstration showed you that, too. This is, remember, the slide he used to show what he called a typical VPN, and here you have what he called a private source address and a private destination and a message: Cut our prices today.

And what happened is that private or true address got put into an encrypted wrapper right there, and only an outer address was visible. Not the true private address. That was over here in the encrypted packet.

So what any hacker could see was not what's in this yellow box but the fake address is on the outside, just like the book that Dr. Jones used at his class at the University of Tennessee. Exactly the same approach.

The true IP addresses were scrambled. That's one way you could have hidden it. Also, Microsoft doesn't do that.

The patent tells you another way you can hide it. He says you can -- the true destination address is concealed, and he describes that in Column 3. But we don't do that either. It's not concealed. It's plainly visible.

Now, they also talk about those degrees of anonymity. Remember that cross-examination?

And the patent doesn't talk about degrees of anonymity. It says: Can you tell whether computer one is talking to computer two, and if the answer is yes, there's no anonymity.

And Dr. Jones was forced to admit to that. Anonymity means you can't determine the identity of the computers that are taking to each other.

He also agreed that the CIA wouldn't be too happy with something like our product, which has the IP addresses visible, which is just common sense. And you've heard over and over again how they're trying to make this something that would be anonymous to the CIA and their agents sitting in remote places around the world.

Our products are being used by people in coffee shops. It's not for the CIA. That's the reason it's not anonymous in the same way their patents are talking about. Their patents were designed for a totally different purpose than the Microsoft products are being used for that are being accused.

But even more than that, Dr. Jones admitted the reason why the CIA wouldn't be happy. From an IP address, which is plainly visible in our product, you can learn the information about where that machine is and what's going on. It's not anonymous at all. He conceded that.

The next argument was SIP addresses, that the SIP addresses are concealed. And he's right. That's true. But those SIP addresses correspond to people, not machines. And he agreed that you had to be anonymous as to the machines.

And, in fact, that's what the patent says. Column 1, the very first column of the patent where it's talking about anonymity, it doesn't say you want to prevent the person from being identified, although you probably want that, too. It's the machine. And the SIP address has nothing to do with that.

Under their theory, you could conceal my name but put my address out on the internet, and that would be anonymous. Doesn't sound very anonymous to me. They can find me. And they can do that with an IP address, too, which is exactly what Dr. Jones admitted.

So on VPN, there's no VPN. That's a requirement for all claims. No infringement of any claim if VPN is not there, and it's not.

The second issue on '135 is the website. Here it's admitted that there's no website. So now we're just talking about whether this OC server is equivalent to a website.

Now, this testimony was absolutely unrebutted from Dr. Johnson. He showed you all of the things that are important about a website and all of the things that are important about OCS, and they just simply don't overlap.

Now, you he heard counsel for VirnetX say that Dr. Johnson had to admit that he was wrong. He didn't admit he was wrong. He was marking out X's no matter what Dr. Johnson said. He disagreed with them on the stand and said, I disagree with you, and he still put an X to the testimony. That's words, not facts.

Now, here's what Dr. Jones did say, and it's important. He said: Well, I think they're equivalent, because of this function-way-result test. And that was in the instructions that Judge Davis just gave you.

But when you read his testimony, basically, he's saying any VPN is equivalent. Well, we know that can't be true, because they didn't invent VPNs.

He says: Well, the function is, you use computers and a VPN to present information to clients, and the clients are authorized. And then he was forced to admit that every VPN does that.

Well, what was the way on function-way-result? Well, you use computers and a VPN to present information.

So if function and way are the same now, what's result? Well, you communicate with computers and a VPN and only clients that are registered.

All right. So it's all the same.

And then I asked him over and over again, every VPN does that, doesn't it? So, basically, you're saying every VPN is covered.

And he said: Well, yes, any VPN meets that requirement. That's typical on VPNs; typical of VPNs; typical of VPNs.

So what he's saying is, he wants them to get paid for anything that's a VPN. But they've admitted they didn't invent VPN. So that's not supported here.

So on the '135, two requirements are missing. Even if only one is missing, there's no infringement.

The '180 patent, two missing: VPN, we've already talked about most of that, and no secure computer address, both requirements of the claims.

The PeerNet software, exactly the same issue. They can see exactly the same thing. On the PeerNet software, you have a one true address, not a separate address, and a one true address over here, and the hacker can see that. And there's no dispute about those facts.

So what do they say? They say: Well, you can't see the groups. That's what the claim says. And look at what the patent says, if the patent says we're concerned about groups. It says, no, we're concerned about anonymity between whether computer one is in communication with computer two.

And the same holds true with the OC issue. Remember when Mr. Cawley, in closing argument, said, let's add all these other computers at the other side of the slide on OC?

That's not what the claim is talking about. The claim is saying computer one talking to computer two. Computer one was the computer on the left; computer two is the OC server. And the hacker can plainly see that, plain as day.

The second issue is no computer has a secure network address. Judge Davis' instruction is that an address requires authentication for access. So let's look.

This computer -- you remember this demonstration from the testimony -- has one address, and it's not secure because anybody can send spam e-mail or anything else into that address even when a Windows Meeting Space session is in play.

So the application might be secure, you have to log in for an application, but the address is not. And that's what the claim requires: A secure address.

Mr. Cawley says: Well, you could have a communication line coming in, and he shows you the patent.

Remember the address, though, was different. One was .com, and one was .scom. Here it was talking about a single address, and it's not secure, because any spam calming into that e-mail can come right in.

So that's the first issue: Does

Microsoft's software use the VirnetX's patents? The answer to that is no. We don't have the anonymity that's required because we're using it for different purposes. It's not a secure computer network address. And it's not a website or an equivalent to it.

The second: Was VirnetX first. This is issue -- part of the issue of validity. We showed you extensive evidence.

But even they knew they were in trouble from the very beginning. This is a presentation given to the CEO, Dr. Beyster, of SAIC that Mr. Munger had presented and prepared.

He said: Wow, there's a lot of companies addressing the issue that we're talking about. The race is on. They were in a race, and they knew it, and that's the same issue cited here. Who won the race?

Was VirnetX first when it filed its patent in 2000, or were others first? And the answer is others were first.

Mr. Munger may have had this realization in the late 1990s when he was working on Global Hawk, and he may have thought that he could try to solve that problem. The problem is that others who were working in this space before had had that same realization many, many years before, and they had the same solutions many

years before. That's why he wasn't first.
SAIC's date is over here in 2000.
PPTP, invented by Mr. Pall, was four years earlier in '96.
AutoDial, also in '96, four years earlier.
DVPN from TIS, that was in 1998, two years earlier.
Aventail, one year earlier.
They didn't win the race, and yet that's exactly the issue the Court is asking you to decide, who was first?
Now, you might say: Why is it -- why is all of this relevant? Why didn't the Patent Office find it? We showed you that earlier. The Patent Office did not consider this material, and there's no dispute about that, none at all.
So when counsel for VirnetX says the presumption of validity applies because the Patent Office is presumed to have done its job well, it did its job well with the information they had, but they didn't have any of this information that you're seeing.
In the video and all the witnesses agreed, this is your task. This is your job to decide. You can't defer to the Patent Office and say they must have decided this is okay, because they didn't have the same

information.

And when you hear counsel for VirnetX say over and over again with every witness, there's a presumption of validity, that's a suggestion that you really shouldn't have to look at this too hard.

Doesn't reduce how hard you have to look at it at all, because the Patent Office has not looked at this at all. You will be the first, and you'll be the only to decide this question.

Aventail. Aventail, we know they lost the race, and we know that Mr. Munger and Dr. Short knew they lost the race, because SAIC, their own employer, chose Aventail over Mr. Munger's technology. They had a choice as to what to use with ANX, and they said let's go with Aventail. It's better. It works. And they invested in Aventail as we talked about earlier. So they lost the race to Aventail very clearly.

Aventail: Secure, authenticated access to a customer's critical software application, exactly how they described their invention to you here over and over again. It's automatic. It's being used by a number of Fortune 100 companies. It works. It's automatic. It's easy. All of the things that they claim to have invented were done by Aventail earlier and better.

Large virtual private networks. You heard that -- you heard them argue that Aventail is not a private network. Well, large virtual private network. Everybody else in the world is calling what they're doing a VPN. Only VirnetX.

You heard Dr. Wicker transparently and automatic. There's no debate that they do exactly what Mr. Munger and Dr. Short claim, but they did it earlier.

So what does Dr. Jones argue? He argued to you today: But it's not a network. Well, how can it not be a network when over and over again, not only Aventail is saying it's a VPN, a virtual private network, but everybody else is calling it a network, too, including SAIC.

Mr. Munger's own employer says: Well, VPN system providers, and they list Aventail as the very first one. So the only people not calling Aventail a network, a VPN, is VirnetX in front of you. But their employers and everybody else acknowledges that's exactly what it is. And that's Exhibit 382, one of the Plaintiff's exhibits.

The next piece of prior art is the PPTP, what Mr. Pall invented in 1996 with AutoDial, way before, four years before, and improved on even twice before the work that Mr. Munger and Dr. Short did.

Recognized by everyone as a break-through four years earlier. A new protocol secure remote access across the internet, a great virtual private network or VPN. Four years earlier.

Automatic. Automatic. Easy. Easy. Easy. You heard that testimony over and over again.

So what's the first point that you hear raised? Well, it only reconnects. That means it's -- the second time you call them up, it does it automatically.

And you heard the arguments, well, why didn't they show you the first time that they connected them? And without arguing about the demonstration, did you see Mr. Munger or Dr. Short show you how they connected the first time on their demonstration? No. No. But it was one click for each, exactly the same setup, exactly the same, but four years earlier for PPTP with AutoDial.

So what does Mr. Jones say? He says there's not a determination step. And, in fact, Professor Wicker explained to you in detail why there's a determination step.

And you heard Dr. Jones today on the stand admit that what happens is that the system looks up at the address book and says, is there an entry? And if there's an entry, it determines that it should use PPTP.

PPTP is actually in the phone book entry. You heard him admit that this morning. That's exactly where the determination step happens. If it's in the phone book, it says use PPTP. If it's not in the phone book, it goes off and forms a different path. Dr. Jones admitted that this morning in this courtroom.

Now, you heard them talk about the false step demonstration that was given with eBay and this-is-not-a-secure-website.com. Well, that doesn't work either, because -- Dr. Wicker explained, because the only reason that it happened that way in this demonstration is they picked a bogus name in thisisnotasecurewebsite.com.

And as to eBay, which is not a bogus name, it wasn't connected to the internet, so it couldn't find it.

So those demonstration examples that they did on cross-examination weren't applicable, and he explained that in detail.

And this is the phone book entry that I was talking about earlier where it says -- it's sort of hard to see here, but it says: PPTP. That's what Dr. Jones had to admit on cross-examination today, that if that is there, the phone book entry, that's determining.

Now, one of the things you heard in cross-examination was, well, wait a minute. How can PPTP be private and anonymous if Office Communicator isn't? Because you can still see some IP addresses. And there's no doubt you can see IP addresses, but you can't see the private IP addresses that Dr. Short admitted were there.

And so let's take Office Communicator first. That true source sending to that true destination has one and only one IP address, and that's visible plainly in what that hacker can see.

On PPTP, what that's -- what's visible are the IP addresses of these two boxes, not the real source, not the real destination. Mr. Pall explained that. Dr. Wicker explained that. The addresses of the true source and true destination are in this encrypted packet. The hacker cannot see it. That's why it's different.

And PPTP, it's anonymous because they're encrypted. And Office Communicator, what they're accusing of infringement, they're plain to see by anybody out there, like Dr. Jones admitted.

The last piece of prior art I want to talk to about is DVPN or Dynamic VPN. That was a product developed by Trusted Information Systems and demonstrated at DARPA, well before any of the work that they -- that Mr. Munger and Dr. Short ever talked about. So they lost that race, too.

You heard from Mr. Saydjari, 17 years with the Department of Defense. He's the man who's actually responsible for cyber security in the United States. He's the one who was actually responsible for trying to maintain our security and deciding which technologies would do that best.

He represents reality. He doesn't have any dog in this fight. And he came here to say what actually happened at that conference in March of 1998.

And what happened? It was a successful demonstration. In fact, unqualified success. The documents -- not just people's recollection, but the contemporaneous documents were also very, very clear and undeniable.

Automated VPN. Automatically activate the VPN. Exactly what Mr. Munger and Dr. Short claimed they invented, VPN did before. That's automatic activation.

And was it easy? Yes. Mr. Saydjari said that was a requirement. Remember he said we want to do this with coalition forces when we're sitting over in Iraq someplace, and we have to deal with the British forces and the German forces and the Belgium forces and other forces. We have to be able to communicate securely with everybody. That's what this is for. It's real world, real facts, real life. So it had to be easy.

Did it work? You bet. Absolutely critical, great success in that way. Demonstrated it a year before -- two years before the relevant time period of Mr. Munger and Dr. Short.

Now, did DARPA fund the SAIC and Mr. Munger's VPN invention? Because, remember, Mr. Munger submitted a proposal directly to Mr. Saydjari saying: Please fund my technology instead of others.

And Mr. Saydjari didn't -- as I say, didn't have a dog in that fight. He's going to decide what's better and what works. That's his job. And he said: No, we didn't fund it.

Why? It was a duplicate of what we had already created with DVPN technology. They lost the race with DVPN, too.

Now, the cross-examination of Dr. Wicker on DVPN was interesting. Over and over and over and over again, the VirnetX lawyer said: Well, do you know with absolute certainly what happened 12 years ago?

And Professor Wicker said: Well, I wasn't there, so I guess I don't know with absolutely certainty almost anything, but I think it's clear and convincing.

That, of course, is the standard that Judge Davis just instructed you on.

Again, well, is it -- are you absolutely certain?

Well, no, but I think it's clear.

Judge Davis' instructions told you proof to an absolute certainty is not required. But over and over and over again, VirnetX's counsel was trying to suggest that that is the standard; that if Professor Wicker is not absolutely certain, you shouldn't rely on him. But that's exactly the wrong statement.

So was VirnetX first? No. They lost the race to Aventail; they lost it to DVPN; and they lost it to Mr. Pall, four years late, on PPTP.

Obviousness. Mr. Wicker testified at length about obviousness, told you why it was obvious and told you why all the people who were looking at this in detail sitting in the Engineering Internet Task Force would know why this is obvious.

Now, Dr. Jones spoke about obviousness for about to two minutes, maybe a minute and a half. And always said, well, you can't use hindsight, and Dr. Wicker didn't. He showed you at the time why everything they're claiming was known, because we had a lot of very smart people working on this problem for a long time, and they were working together to make that work.

The objective considerations that are in that long list that Judge Davis says he would leave to you to read when he was reading the instructions, remember Dr. Wicker went quite through and showed how those considerations showed absolute obviousness. Their expert, Dr. Jones, didn't respond to that at all. At all. Didn't even mention it.

Now, you've heard many, many times this presumption of validity. But the presumption can be rebutted. You, the finder of fact, can find the patent to be invalid. That's from the Court and also from the video.

It's important that you understand your role in the process. You will be the first people to decide this question. And any suggestion that you should look at this with less rigor or with less scrutiny because of the presumption of validity is asking you not to do your job as jurors.

And that's wrong. The presumption of validity does not change the fact that jurors have to look at this evidence that the Patent Office didn't see.

So was it obvious? Yes.

Willfulness: Objectively high likelihood that the actions infringed. Well, what evidence do we have on this?

First, SAIC -- VirnetX relies on the letter from Pam Bumann in May of 2006. Talked to you about RFC 3263. Well, that's the one that Mr. Larsen admitted was wrong.

How are we supposed to know objectively that we infringe when they can't even get it written in the letter? They say you infringe because of X, and X is false. It's not objectively true even under their theory.

Do they correct that? Do they send us any information? No.

How can it be objectively true when their own inventor, Dr. Larson, said: No, I haven't changed my mind. My patents offer, as he put it, no protection against what Microsoft is doing.

How can -- objectively, we're supposed to know we infringe when their own inventor and Mr. Larsen don't?

So also on willfulness, does Microsoft just say: Forget it; we didn't want to talk to you; we're not interested; we don't care; go away; file a lawsuit; we're big; we're powerful? No.

04:23 They said: Let's have a meeting and discuss it, but please provide us the information that supports your claim.

04:23 Everybody in this courtroom has admitted that's a reasonable thing to do.

04:23 Did SAIC and VirnetX give us any information to back up the claim which later turned out to be false? No.

04:23 Did they do anything to set up a meeting? No.

04:23 Mr. Larsen, do you know whether Ms. Bumann set up a meeting?

04:23 Can't speak for her.

04:23 He sure didn't. There's absolutely nothing suggesting that any such meeting occurred. And this Bumann member even said that she didn't get the letter. That was her reason, that was her explanation for why she didn't even send the letter.

04:24 So patent review policies. You heard this in closing argument just a minute ago. That Microsoft -- you should be shocked. VirnetX's lawyers asked you if you were shocked that Microsoft doesn't go look at patents.

04:24 Well, Microsoft explained why. If you're writing a song and you're creating it yourself, you don't need to go look at patents. We want people to innovate.

And he said: Well, and if somebody shows us that we're -- that we might be using their technology, we go out to them and license it.

That's not the voice of a willful infringer. That's somebody who's reasonably respecting intellectual property.

But now let's look -- put the shoe on the other foot.

Mr. Munger, well, wait a minute. When you're going out to work on Gabriel, do you look at other people's patents?

Mr. Munger, well, he wasn't shocked when he learned about it, because he doesn't do it either. VirnetX has no policy saying you should go look at anybody's patents.

Dr. Larson, he says, well, why didn't you do an analysis of other people's patents.

He says: It doesn't even make sense to me.

So if VirnetX's lawyer is suggesting you should be shocked about it, their own people say it's standard.

Last issue: The Patent Office.

Say, Well, Microsoft got a notice from the Patent Office about Mr. Munger's patent. True. But did they go to the Microsoft? No. It went to a law firm. No evidence that anybody at Microsoft ever learned about it.

And the Patent Office issued the patent over it, as I showed you earlier.

Now, damages. Defendants never like to talk about damages, but I have to. Our view is the damages are zero. The damages are zero, because there's no infringement, and the patents are invalid.

Well, now I'm going to assume for a minute that you disagree with me, and let's talk about what those damages should be.

The Court tells you they can't be remote or speculative. Those were the instructions you just got. And this is the real evidence they relied upon.

They said: Well, these are the benchmarks. Remember Mr. Reed said: These are the key licenses you look at, and he pointed to these high rates.

What he didn't point out was there was absolutely zero dollars under any one of them. Their benchmarks for the value of this technology and not -- a dime wasn't paid under those royalties.

Hypothetical negotiation, what everybody talked about would have occurred in 2003. They're saying that at that negotiation, Microsoft would have said: Here's $242 million.

Well, what would have happened? What had happened already is that SAIC would be coming into that negotiation being told by the CIA that their technology is in the living dead category. Their own company hadn't pulled the plug because the product's not worth investing in.

They go to 32 venture capitalists, and everybody else in the world who says: Sorry, your technology is worth nothing.

SafeNet terminates and doesn't pay them a dime.

And what Mr. Reed and VirnetX is saying is, just a couple of months later, SAIC would have been so confident about the strength of its technology that they would have held out to $242 million. That was his testimony.

And you remember when Mr. Sayles was asking him questions, he said: Well, if Microsoft had offered at that hypothetical negotiation 10 million, they would have gotten up and left?

Absolutely would have.

15 million?

Without a question, they would have gotten up in a huff and walked out of the room.

Well, there's two problems with that. One is, he admitted that part of the deal of a hypothetical negotiation is you can't walk away.

The other problem is it violates common sense. Here you have a company that's spent years trying to get someone to give them millions, 2 million, $3 million, 7, being told no everywhere they went, and all of a sudden, Microsoft would offer them 5, $10 million, and they would throw a fit and leave? It just doesn't make sense.

It also is inconsistent with all the evidence in the case about the entire value of the company, not just these patents, the entire value of the company, which consistently across the range is between the 15-million-dollar range.

And yet all around the hypothetical negotiation time, before and after the patent issues, and yet they said: You really ought to say now it's worth $242 million.

The reason this bar is so high and these bars are so low is that these bars reflect their best estimate of the value of the entire company. This bar represents what Microsoft contributed, and they're trying to take that.

Now, you heard this morning about CSMG, a company that said: Hey, if your technology really works, there's a huge opportunity out there. It might be worth $200 million.

It didn't say the technology was good. It didn't say the technology was actually worth that. It said, if the technology sells like hot cakes, then you could make that amount of money. That's what that document says.

So in terms of the actual verdict form, we, obviously, have a different view as to how we would ask you to fill it out. We believe that in the question of infringement, the answer should be no. Website, VPN, secure network address.

Willfulness? No, they failed to meet their burden of proof. We asked them for a meeting, and they didn't even show up. We asked them to give us some information to back up the claim that turned out to be false. They didn't give it.

Invalidity? Yes. They lost the race to three different companies, all of which provided fast, easy, automatic ways of connecting VPN years before Mr. Munger and Dr. Short.

Damages? Zero.

Remember this slogan? This was the log-in box that was on the Gabriel prototype, that Mr. Munger had to put in, that Dr. Short had to put in, everybody had -- when they were going to put in to work on Gabriel at all, the number, the password they had to put in was Microsoft for money in 2009, question mark.

Now, that's tells you more than almost anything I could say about what this case is actually about. That's what this case is about.

And you heard, well -- Mr. Munger said: Well, that was just in there for a couple of weeks. Well, it turns out that's not true.

Dr. Larson, who testified by video this morning, said: Well, he's the one who actually put it in there.

And where did he get it? He says: I copied it from one of my other passwords that I use as a standard password for other developers.

So all of -- all of VirnetX was saying this lawsuit, Gabriel, everything is just about whether we can get money out of Microsoft. Microsoft and money, now that we're in 2010, we suggest the answer to that question should be no.

Now, this is my last opportunity to speak to you. Many times in trials, there's cheering and applause when that happens. But I do -- and Mr. Cawley will have a few minutes to respond to what I'm saying, and I won't be able to answer it.

But I want to ask you to please listen to see if he answers these questions. Not talk about Global Hawk, Purple Hearts, or scud missiles, but the questions that are in the case and see if he answers these questions.

First, why did everybody refuse to buy or invest in the VirnetX technology if it really worked, if it really did what they say it does?

If it was really worth $242 million, why did 32 venture capitalists, every company, every government agency, SAIC, the CIA, In-Q-Tel, SafeNet, everybody, why did everybody with motivation to invest or buy it, to use it if it worked, say no?

Ask for an answer to that question that makes sense to you.

Would the CIA use software that doesn't provide anonymity? Their own expert, Dr. Jones, said no. They told you over and over again that's what they were trying to do: Create software for the CIA.

Well, that's not what Microsoft is creating. We're creating it for normal people using it for normal things.

What was first? Was VirnetX before Aventail? Before VPN, but before DVPN? You heard no denial from Dr. Jones. Dr. Jones testified on the stand today -- he didn't deny that Aventail, VPN, or PPTP were all fast, automatic, easy. And I pointed that out to him on cross-examination, and he didn't deny that.

How can VirnetX demand 20 times, 20 times what SAIC and the missing Kendall Larsen thought the entire company was worth? Does that make sense? Does that make any sense at all? That's just way, way too high. And we all in the courtroom know that. Twenty times clearly shows that they're trying to get the value Microsoft contributes, not that they contributed.

And last, where is Kendall Larsen, if he's the President, the CEO, Chairman of the Board, founder, the largest stockholder, and he said some things that are critical to this case that show there's no infringement and no validity?

He's the one that stands to make the most out of this lawsuit, and he didn't have the guts to come and stand before you and ask that and defend that. And that tells you a lot about what this case is about.

I thank you very much for your attention and respectfully ask that you enter a verdict for

04:33 Microsoft.

04:33 THE COURT: Thank you, Mr. Powers.
04:33 All right. Rebuttal, Mr. Cawley.

04:33 MR. CAWLEY: Thank you, Your Honor.

04:33 Ladies of the Jury, what I want to do in 04:33 the last 10 minutes, what I said I would do, Mr. -- 04:34 Microsoft's lawyer had had some questions he thinks I 04:34 should spend 10 minutes answering.

04:34 And I think we will touch on some of 04:34 those, but I think it's more important at the very end 04:34 of at least the lawyer part of the trial that we focus 04:34 on the questions that Judge Davis is going to ask you. 04:34 His questions, I'd suggest, are the important ones and 04:34 the ones you'll need to really wrestle with in deciding 04:34 the case.

04:34 First of all, let's talk about Kendall 04:34 Larsen. Why isn't he here? Well, there's several 04:34 reasons. First of all, Mr. Larsen is not an inventor of 04:34 these patents. At the time Mr. Munger and Dr. Short 04:34 came up with their invention, they didn't even know 04:34 Kendall Larsen.

04:34 Kendall Larsen did meet them later. He 04:34 believes in the invention. He helped them start a 04:34 company and helped them raise money and invested quite a 04:34 bit of money in himself for -- in it himself. I don't see why there's anything wrong with him getting a return on that investment when he's the one that helped Mr. Munger and Dr. Short be able to come here and enforce their rights against Microsoft's infringement.

And remember, anyway, isn't this just a red herring? Mr. Larsen's deposition got taken. He was on videotape. You saw that played this morning. Microsoft had an opportunity to ask him any questions they wanted and to play for you any of his testimony that they thought was relevant.

They talked about Magenic. Remember how strange and mysterious it was that Mr. Larsen wasn't here to explain why if he thought that Microsoft was already doing what the patent said; he was hiring this company Magenic to put the invention in the Microsoft products?

Mr. Munger explained all that, and that's not the way it happened at all. What he told you is that he and Mr. Larsen had decided that it would be a good idea to show that their invention could be used with the Microsoft products, but they didn't know Microsoft was already using their invention.

That's how Mr. Munger explained to you, in 2005, someone he was working on that said, Come in here and look at this computer screen. It looks as though

Microsoft is already doing what we're trying to do with the invention.

Dr. Vic Larson, you saw him this morning. His deposition was taken in this case. As much as we would have loved to have brought the co-inventor here to testify to you live, we have to cut back somewhere due to time constraints.

His deposition was taken. Microsoft had an opportunity to ask him any questions they wanted and play for you any of the testimony that they thought was relevant.

SAIC and Pam Bumann, same thing. Her deposition was taken. They could have played any part of that deposition they wanted to.

So let's talk about the first question that Judge Davis is going to ask you. Is there infringement? Once again, you heard about this question, is it anonymous?

But remember that slide -- I won't take the time to put it up again -- where Microsoft tried to show you the envelope and said the hacker or spy could see the address on the envelope?

But I'll be darned if they didn't do again what Dr. Johnson did you in the first place: They only showed you half of the story. They showed you that you could see that address that goes across the internet and you could see the destination of the server computer, but you can't see the address of the person that it's intended to reach. That's why it's anonymous.

You didn't even hear them address anonymity in PeerNet where you remember the document said it is beyond suspicion that when Microsoft's group sends a message and you can't tell which group member it is, that is anonymity beyond suspicion.

And they say again, well, website. We don't really meet the website limitation of the claims. But remember, Dr. Jones testified to you and explained while how a website is not substantially different from what Microsoft does, he explained how it's not different and explained to you the function and way and result test that shows under the Doctrine of Equivalents that there is still infringement.

And despite what Microsoft's lawyer attempted to tell you, Dr. Johnson sat on the stand and admitted to you under Mr. Caldwell's questioning that he had been wrong when he told you that it was substantially different, when he told you that it wasn't at all the same.

Second question: Is Microsoft's infringement willful?

Well, where was the witness who came to court and explained why Microsoft believed, when it got that letter in 2006, that it didn't infringe?

Where was the witness who explained how Microsoft studied that patent and reached a good-faith conclusion that it didn't infringe? You never heard that testimony because Microsoft has given you no excuses for why it continued to infringe the patent from 2006 until now.

And as far as -- there was some -- some confusion you just heard, remember, about the shock of what Microsoft told its employees. It wasn't necessarily shocking that they don't go out and do a bunch of research. But what that Microsoft developer told you is they are instructed not to read patents. And I suggest to you that's a very different thing.

On the third question: Are the issues of the patents invalid? On the Windows NT demonstration that you were shown, if it's easy to set up a PPTP connection the first time, why didn't they show you that? Dr. Short showed you that but Mr. Pall didn't, and he didn't because of the complexity of setting up that system for the first time.

And what about the BIOS software? It was repeated again to you just now. Oh, all that software was from 1996. The BIOS software was from 2000. Some of the software running on his computer was running Windows 2000. We heard that this morning.

And the attempt to communicate to eBay, which I asked Mr. Pall to do, well, they pointed out to you, and maybe quite correctly, they couldn't communicate with eBay because they didn't hook their demonstration up to the internet.

Why is that; do you think? Dr. Short did. We know that the Court provides internet connection in this courtroom. You saw Dr. Short using it. Why wouldn't Microsoft give its demonstration to you using a realistic internet connection?

DVPN. Mr. Sterne testified by deposition, but he said he didn't know what was in that demonstration. Mr. Kendrick, the same thing. The only person you've heard from who was at that demonstration was Mr. Saydjari, and he testified to you he wasn't sure what was demonstrated and he didn't think they used a DNS trigger as the patent called for.

And Aventail, the evidence is undisputed that Aventail is point-to-point and that that is not a VPN by Judge Davis' definition.

The documents you saw in which people in 2002 or so described Aventail as being a network, as being a VPN connection, they didn't have Judge Davis' definition about what that phrase means in this case.

And finally, how much is a reasonable royalty? Consider these facts: There was a recession in 2001. It mostly affected tech companies.

Mr. Munger explained to you how at the time he came up with this invention, most people were using slow dial-up connections and not the rapid connections that they have now.

In short, although the seed of his invention had been planted, the tree had not yet grown because the need had not yet developed in the way that it would in the next few years.

But Mr. Munger never told you that he couldn't raise money because of 9/11. He told you that he was distracted by working at the FBI headquarters for a year.

And finally, there was this strange discussion about the timing is not right because that they -- they couldn't get money in 2001 and Microsoft didn't start using it in 2003.

The timing is perfect. The whole point of it is that although Mr. Munger and Dr. Short kept on comin' and kept on trying, by the time there was a major demand for their invention, Microsoft was already using it.

And once the largest software company in the world starts using your invention, you, as a tiny company, are going to have very little opportunity to go out there and compete with them unless they're made to respect your patent rights.

And finally, did we suggest to you that the negotiators with Microsoft in this hypothetical negotiation in 2003 would have held out for $242 million? Not what anyone said at all.

What Mr. Reed suggested to you is that Microsoft and the owners of the patent would have agreed to a royalty of one-third of a penny for the sales that Microsoft would make in the future.

What he also testified is, if you go back and do the arithmetic, which, of course, no one knew at that time, but today, because of the enormous amount of money that Microsoft has made from using this invention, that number would come to a total of $242 million.

THE COURT: Mr. Cawley, your time's expired.

MR. CAWLEY: Thank you.

Ladies of the Jury, I appreciate your attention. This is now your time to write the last chapter of this story, and we look forward to your answer.

THE COURT: Thank you, Mr. Cawley.

All right, Ladies of the Jury. It's almost 5:45. We're about to send you to deliberate. As you'll recall, a week ago we started. You've heard the opening statements, all the evidence, the Court's charge, the closing arguments of counsel. So now is the time that you can go to the jury room and begin your deliberations.

I have a few instructions to give you in that regard.

First of all, only deliberate if all eight of you are in the room. If someone has to leave the room for a moment, please stop deliberating. And the reason for that is important. Everyone needs to hear everything that everyone else has to say. So follow that instruction during your deliberations.

If you need to communicate with me, again, send a note. If you wish to recess this evening and resume tomorrow, please send me a note before you do so advising me of your plans and outlining what you intend to do.

Then I will send you a note back confirming that that is acceptable, which I'm sure it will be.

Again, if you do recess tonight, please follow my instructions. Do not discuss the case with anyone else. Do not discuss the case among yourselves unless you're all together and make no independent investigation.

On behalf of all the parties and the Court, I want to thank you immensely for your sacrifice of time, energy and attention here this week hearing this case. And you are now released to the jury room to begin your deliberations.

COURT SECURITY OFFICER: All rise for the jury.

(Jury out.)

THE COURT: Please be seated.

All right. Is there anything further from the Plaintiff?

MR. CAWLEY: I don't think so, Your Honor.

THE COURT: Okay. From the Defendant?

MR. POWERS: No, Your Honor.

THE COURT: All right. Thank you.

Let me just congratulate both sides for a very well tried case from both sides, and we'll be in recess awaiting the jury's verdict.

COURT SECURITY OFFICER: All rise.

(Jury deliberations.)

(Jury out.)

COURT SECURITY OFFICER: All rise.

THE COURT: Please be seated.

COURTROOM DEPUTY: Judge, I have them here somewhere.

THE COURT: Excuse me?

COURTROOM DEPUTY: Your notes, did I put them on the bench?

THE COURT: Yeah, I've got it here.

All right. I have a note from the jury that just states, We've selected a fore -- foreman.

I don't know how they did that, but...

We will be leaving tonight at 6:30 p.m. and reside -- resume -- I guess it says reside. I guess that means resume tomorrow at 9:00 a.m. Thank you. Signed Laura Warr, Jury Foreperson.

So I'm going to send a note back to them that just says, That will be fine. Remember my instructions. Wait until everyone is in the jury room before you begin in the morning. Have a nice evening.

Any objections?

MR. CAWLEY: No objection from Plaintiff, Your Honor.

MR. BOBROW: No objection, Your Honor.

THE COURT: All right. Now, I'm going to

-- I'll send this note back in, but they do plan to deliberate for another 30 minutes, and so they will be leaving around 6:30.

So I'm going to ask around 6:30, if you're here, an attorney or anybody in the audience, either be gone home by then or be in the courtroom by then so that the jury can exit without encountering anyone.

And the same thing in the morning. They're going to start back at 9:00, so they'll probably be here by -- you know, start arriving at a quarter till. So I'll say if you wish to be here in the morning, arrive and come to the courtroom before 8:45 or come after 9:10 to just allow the jury unfettered access.

So I will be here until 6:30, but we won't resume unless the jury has another note between now and then.

MR. CAWLEY: Will someone let us know when they've left?

THE COURT: We will. We'll let you know when they leave.

MR. BOBROW: Thank you.

THE COURT: Very well. Be in recess.

COURT SECURITY OFFICER: All rise.

(Jury deliberations continued.)

CERTIFICATION

I HEREBY CERTIFY that the foregoing is a true and correct transcript from the stenographic notes of the proceedings in the above-entitled matter to the best of my ability.

/s/______________________________ ________________________
SUSAN SIMMONS, CSR Date
Official Court Reporter
State of Texas No.: 267
Expiration Date: 12/31/10

/s/________________________ ____________________
JUDITH WERLINGER, CSR Date
Deputy Official Court Reporter
State of Texas No.: 731
Expiration Date: 12/31/10

EXHIBIT G

Attorney Docket No. 077580-0090

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:	)
Edmund Munger, et al.	)
	)
U.S. Patent No.: 7,188,180	)
Filed: November 7, 2003	) **Examiner:**
Issued: March 6, 2007	) **Andrew L. Nalven**
	)
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	) **Group Art Unit: 3992**
	)
Reexamination Proceeding	)
Control No.: 95/001,270	)
Filed: December 8, 2009	)

CERTIFICATE OF SERVICE

WE HEREBY CERTIFY that the Declaration of Jason Nieh, Ph.D., Pursuant to 37 C.F.R. § 1.132, filed with United States Patent and Trademark Office on April 19, 2010, was served this 19th day of April, 2010 on Requester by causing a true copy of same to be deposited as first-class mail for delivery to:

William N. Hughet
Rothwell, Figg, Ernst & Manbeck, P.C.
1425 K Street N.W.
Suite 800
Washington, D.C. 20005

Respectfully submitted,
McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/
Toby H. Kusmer, P.C., Reg. No. 26,418
Matthew E. Leno, Reg. No. 41,149
Hasan M. Rashid, Reg. No. 62,390
McDermott Will & Emery LLP
Attorneys for Patent Owner
Please recognize our Customer No. 23630 as our correspondence address.

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com,
mleno@mwe.com
hrashid@mwe.com
Date: April 19, 2010

BST99 1648163-1.077580.0090

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:	)	
Edmund Munger, et al.	)	
	)	
U.S. Patent No.: 7,188,180	)	
Filed: November 7, 2003	)	**Examiner:**
Issued: March 6, 2007	)	**Andrew L. Nalven**
	)	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	)	**Group Art Unit: 3992**
	)	
Reexamination Proceeding	)	
Control No.: 95/001,270	)	
Filed: December 8, 2009	)	

Declaration of Jason Nieh, Ph.D., Pursuant to 37 C.F.R. § 1.132

Pursuant to 37 C.F.R. § 1.132, I declare that the following statements are true to the best of my knowledge, information, and belief, formed after reasonable inquiry under the circumstances.

Background

1. I have over 15 years of experience with operating systems and distributed systems. More specifically, my experience includes remote access, computer networking, and computer security. Examples of my experience are evidenced by my publication of papers in top-tier networking and security conferences, service on programming committees for networking and security conferences, awards for research work, and receipt of research grants in the field of networking and security. My qualifications, including a description of all of this information, may be found in my curriculum vitae, which is attached hereto as Exhibit A.

2. I earned a Bachelor of Science degree from the Massachusetts Institute of Technology in Electrical Engineering in1989. I earned a Masters of Science degree from Stanford University in Electrical Engineering in 1990. I also received my Ph.D. in Electrical Engineering from Stanford University in 1999.

3. I joined Columbia University as a faculty member in 1999, where I am now a tenured Associate Professor in the Department of Computer Science. I am also currently the director of the Network Computer Laboratory at Columbia University.

4. My research interests include mobile computing, operating systems, distributed systems, thin-client computing, web and multimedia systems, and performance evaluation. I have

supervised a number of Ph.D. students who worked on and completed dissertations in the area of networking and security. I also teach courses in advanced operating systems and mobile computing, both of which involve computer networking and security.

5. I have also served as an expert in various litigations in the fields of computer networking and security, which include virtual private networking.

Resources I have Consulted

6. I have been retained by the Patent Owner, VirnetX, Inc., to offer my opinion of the patentability of claims 1, 10, 12-15, 17, 26, 28-31, and 33 of U.S. Patent No. 7,188,180 ("the '180 Patent") in view of the Office Action dated January 19, 2010 ("the Office Action") received by the Patent Owner in the reexamination of the '180 Patent.

7. In preparing this declaration, I have reviewed the '180 Patent. I have also reviewed the Office Action. I have also reviewed the Request for *Inter Partes* Reexamination of Patent ("the Request") to the extent it is adopted by the Office Action. I have also reviewed Appendices A-H to the Request to the extent that they are adopted in the Office Action. Lastly, I have reviewed the references upon which the rejections in the Office Action are based, namely Aventail Connect v3.1/v2.6 Administrator's Guide ("Aventail"); Microsoft Windows NT Server, Virtual Private Networking: An Overview ("VPN Overview"); IETF RFC 1035 ("RFC 1035"); Kosiur, "Building and Managing Virtual Private Networks" ("Kosiur"); Kaufman, "Implementing IPsec" ("Kaufman"); James M. Galvin, "Public Key Distribution with Secure DNS" ("Galvin"); "Gauntlet® Firewall for Windows NT Administrator's Guide Version 5.0 ("Gauntlet"); "Microsoft Windows NT Technical Support Hands-on, Self-Paced Training for Supporting Version 4.0" ("Hands-On"); "Microsoft Windows NT Server, Whitepaper: Installing, Configuring, and Using PPTP with Microsoft Clients and Servers" ("Installing NT"); and "Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources" ("Microsoft VPN").

8. A detailed explanation of the basis for my opinions is set forth in the remainder of this declaration.

Detailed Basis for My Opinion

<u>Secure Domain Name and Secure Domain Name Service</u>

9. As I stated above, I have read the '180 Patent and understand independent claims 1, 17, and 33 recite a <u>secure</u> domain name and a <u>secure</u> domain name service.

10. As I read the Office Action and the Request, those documents rely on the erroneous premise that a <u>secure</u> domain name is a domain name that just happens to correspond to a secure computer. Alternatively, the Request and Office Action rely on the faulty position that a <u>secure</u> domain name corresponds to an address that simply requires authorization. These assertions are in clear contradiction of the specification to the '180 Patent, which takes pains to explain that a <u>secure</u> domain name is different from a domain name that just happens to be associated with a secure computer or just happens to be associated with an address requiring authorization, as shown in the '180 Patent at column 51, lines 18-32. To illustrate, in various implementations,

the '180 Patent describes that a secure domain name is a "a non-standard domain name." Examples of such non-standard domain names are described in Claim 11: .scom, .snet, .sorg, .sedu, .smil, and .sgov. Dependent claim 2 also differentiates between a secure domain name and a non-secure domain name in reciting the step of "automatically generating a secure domain name corresponding to a non-secure domain name." To further illustrate, the '180 Patent describes, at column 51, lines 28-32, that "a query [with a secure domain name] to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown." Thus, the inventors demonstrated that the secure domain name recited in claims 1, 17, and 33 of the '180 Patent cannot be properly read to be a domain name that just happens to be associated with a secure computer or just happens to be associated with an address requiring authorization. As seen from the previous sentences, a secure domain name is different from a domain name that just happens to be associated with a secure computer or secure computer network address. For example, as pointed above, the domain name that just happens to correspond to a secure computer or a domain name that just happens to correspond to an address requiring authentication can be resolved, for example, by a conventional domain name service; whereas, as noted above, a secure domain name cannot be resolved by a conventional domain name service, for example.

11. Furthermore, even if the recitation "secure domain name" is defined according to the Request to mean a domain name corresponding to a secure computer or a domain name corresponding to an address requiring authorization for access, various of the cited documents still fail to describe or suggest this feature. Specifically, the relied upon portions of the cited documents describe domain names of computers that do not require authorization for access. Instead, the computers (*e.g.*, a VPN tunnel server or a PPTP server) of the cited documents are for securing a connection between a client computer and a target computer. To this end, the computers (*e.g.*, a VPN tunnel server or a PPTP server) themselves do not have a secure computer network address because they do not require authorization for access or authorization for a client computer to communicate with them. Any client computer can, without authorization, communicate with one of these alleged computers (*e.g.* a VPN tunnel server or a PPTP server); it is the target computer that may require authorization for access. Therefore, neither the domain name of the alleged computers (e.g., a VPN tunnel server or a PPTP server) nor their corresponding computer network address is secure – even if this term is defined according to the Request. As such, these cited documents do not teach a secure computer network address or, correspondingly, a secure domain name.

12. Similarly, the Request and Office Action rely on the faulty position that a secure domain name service is nothing more than a conventional DNS server that happens to resolve domain names of secure computers. Alternatively, the Request and Office Action also rely on the faulty position that a secure domain name service is nothing more than a conventional DNS server that happens to resolve domain names of computers that are used to establish a secure connection, such as a VPN tunnel server or a PPTP server. Again, these arguments are belied by the '180 Patent itself. The specification of the '180 Patent, including column 51, lines 29-45 and column 52, lines 4-26, clearly teaches that the claimed secure domain name service of claims 1, 17, and 33 is unlike a conventional domain name service, which the inventors understood as including both DNS and DNS with public key security according to column 40, lines 6-17 of the '180 Patent. To illustrate, the '180 Patent explicitly states that a secure domain name service can resolve addresses for a secure domain name; whereas, a conventional domain name service

cannot resolve addresses for a secure domain name: in an embodiment described at column 51, lines 18-45, the '180 Patent states that "[b]ecause the secure top-level domain name is a non-standard domain name, a query to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown." A secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be associated with a secure domain name. A secure domain name service of the '180 Patent, instead, recognizes that a query message is requesting a secure computer network address and performs its services accordingly. Furthermore, in various implementations, the '180 Patent describes a secure domain name service as providing additional functionalities not available with a conventional domain name service, as described above in the '180 Patent at column 52, lines 4-26. The '180 Patent, at column 40, lines 6-17, even describes the drawbacks of the conventional scheme of a traditional DNS and public key security:

> One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project (RFC 2535).
>
> The conventional scheme suffers from certain drawbacks. For example, any user can perform a DNS request. Moreover, DNS requests resolve to the same value for all users.

Thus, it is my belief that the <u>secure</u> domain name service recited in claims 1, 17, and 33 of the '180 Patent is different from a conventional domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name.

13. Given my statements above, I do not believe that the references cited in the Office Action teach or disclose the <u>secure</u> domain name and <u>secure</u> domain name service recited in claims 1, 17, and 33.

<u>The Aventail Reference</u>

14. After reviewing the Aventail reference, I understand Aventail to disclose a system and architecture for transmitting data between two computers using the SOCKS protocol. The system according to Aventail routes certain, predefined network traffic from a WinSock (Windows sockets) application to an extranet (SOCKS) server, possibly through successive servers. Upon receipt of the network traffic, the SOCKS server is disclosed to transmit the network traffic to the Internet or external network. Aventail's disclosure is limited to connections created at the socket layer of the network architecture.

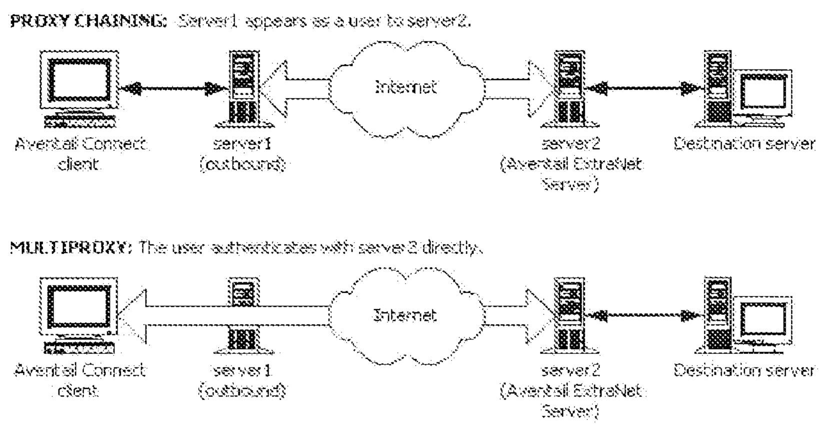
15. I note that pages 9-12 of Aventail discuss the basics of the operation of Aventail Connect, the software necessary to implement the system disclosed in Aventail. According to page 9 of Aventail, a component of the Aventail Connect software described in the reference resides between WinSock and the underlying TCP/IP stack. Accordingly, the Aventail Connect

software is disclosed to intercept all connection requests from the user, and determines whether each request matches local, preset criteria for redirection to a SOCKS server.

16. According to page 12 of Aventail, if redirection is appropriate, then Aventail Connect creates a false DNS entry to return to the requesting application. Aventail discloses that Aventail Connect then forwards the destination hostname identified in the DNS request to the extranet SOCK server over a SOCKS connection.

17. Although Aventail is generally silent on the operation of the SOCKS server, I understand from page 12 that the SOCKS server performs the hostname resolution. Once the hostname is resolved, the user can transmit data over a SOCKS connection to the SOCKS server. The SOCKS server, then, separately relays that transmitted data to the target.

18. Page 12 of the Request, adopted by the Examiner in the Office Action, also cites the "Proxy Chaining" and "MultiProxy" modes disclosed in Aventail at pages 68-73. I have reproduced below a figure taken from page 72 of Aventail depicting these two modes.



19. In the "Proxy Chaining" mode, Aventail discloses that a user can communicate with a target via a number of proxies such that each proxy server acts as a client to the next downstream proxy server. As shown above, in this mode, the user does not communicate directly with the proxy servers other than the one immediately downstream from it.

20. In the "MultiProxy" mode, Aventail discloses that the user, via Aventail Connect, connects through each successive proxy server directly.

21. Regardless of whether one of these modes is enabled, as shown in the figure, an external SOCKS server is necessary and the operation of Aventail Connect, for the purposes of my opinion, does not materially differ based on whether one of these modes is enabled.

22. The Office Action at page 6 asserts that a hostname (*e.g.*, the alleged secure domain name) is secure because this traffic is routed through a SOCKS server and utilizes authentication methods and in some cases encryption. It thus interprets a secure domain name to be a domain name associated with a secure computer. This is incorrect for the reasons I stated in ¶¶ 9-12.

23. The Office Action at page 7 also suggests that a DNS server that can resolve addresses of secure computers corresponds to a secure domain name service. Aventail has not been shown

to teach anything more than a conventional DNS. As I stated in ¶¶ 9-12, however, a secure domain name service cannot be properly read to be a conventional domain name service. A secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name.

24. The Request at page 15 also asserts that Aventail discloses two look-up services, alleged to be described on pages 8 and 12 of that reference. On page 8, Aventail discloses the traditional protocol for a computer to connect to a remote host. On page 12, Aventail discloses "forward[ing] the host-name to the extranet (SOCKS) server [where] the SOCKS server performs the hostname resolution." Here, Aventail has not been shown to disclose anything other than a traditional DNS. As I stated in ¶¶ 9-12, however, a secure domain name service is unlike a conventional domain name service. A secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. As such, Aventail fails to teach a secure domain name and a secure domain name service, as recited in claims 1, 17, and 33.

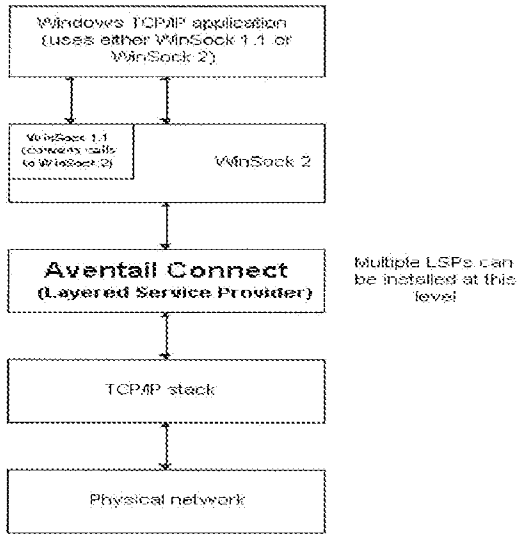
25. Aventail also has not been shown to teach sending an access request message to a secure computer network address using a virtual private ***network*** communication link, as recited in claims 1, 17, and 33. The links created by the systems and methods disclosed in Aventail differ from the virtual private network communication link recited in claims 1, 17, and 33. First, Aventail has not been shown to demonstrate that computers connected via the Aventail system are able to communicate with each other as though they were on the same network. Aventail discloses establishing point-to-point SOCKS connections between a client computer and a SOCKS server. The SOCKS server then relays data received to the intended target. Aventail does not disclose a virtual private network, as recited in claims 1, 17, and 33, where data can be addressed to one or more different computers across the network, regardless of the location of the computer.

26. For example, suppose two computers, A and B, reside on a public network. Further, suppose two computers, X and Y, reside on a private network. If A establishes a VPN connection with X and Y's network to address data to X, and B separately establishes a VPN connection with X and Y's network to address data to Y, then A would nevertheless be able to address data to B, X, and Y without additional set up. This is true because A, B, X, and Y would all be a part of the same virtual private network.

27. In contrast, suppose, according to Aventail, which only discloses communications at the socket layer, A establishes a SOCKS connection with a SOCKS server for relaying data to X, and B separately establishes a SOCKS connection with the SOCKS server for relaying data to Y. In this situation, not only would A be unable to address data to Y without establishing a separate SOCKS connection (*i.e.* a VPN according to the Office Action), but A would be unable to address data to B over a secure connection. This is one example of how the cited portions of Aventail fail to disclose a virtual private network.

28. Second, according to Aventail, Aventail Connect's fundamental operation is incompatible with users transmitting data that is sensitive to network information. As stated

above, Aventail discloses that Aventail Connect operates between the WinSock and TCP/IP layers, as depicted on page 9:



Because Aventail discloses that Aventail Connect operates between these layers, it can intercept DNS requests. Aventail discloses that Aventail Connect intercepts certain DNS requests, and returns a false DNS response to the user if the requested hostname matches a hostname on a user-defined list. Accordingly, Aventail discloses that the user will receive false network information from Aventail Connect for these hostnames. If the client computer hopes to transfer to the target data that is sensitive to network information, Aventail Connect's falsification of the network information would prevent the correct transfer of data. Thus, Aventail has not been shown to disclose a VPN, as recited in claims 1, 17, and 33.

29. Third, Aventail has not been shown to disclose a VPN, as recited in claims 1, 17, and 33, because computers connected according to Aventail do not communicate directly with each other. Aventail discloses a system where a client on a public network transmits data to a SOCKS server via a singular, point-to-point SOCKS connection at the socket layer of the network architecture. The SOCKS server then relays that data to a target computer on a private network on which the SOCKS server also resides. All communications between the client and target stop and start at the intermediate SOCKS server. The client cannot open a connection with the target itself. Therefore, one skilled in the art would not have considered the client and target to be virtually on the same private network. Instead, the client computer and target computer are deliberately separated by the intermediate SOCKS server.

The VPN Overview and RFC 1035 References

30. According to its abstract, VPN Overview provides an overview of VPNs, describing their basic requirements, and some of key technologies that permit private networking over public networks. For example, referring to FIG. 2 of VPN Overview, which I have reproduced below, a VPN is shown to connect a remote user to a corporate Intranet.

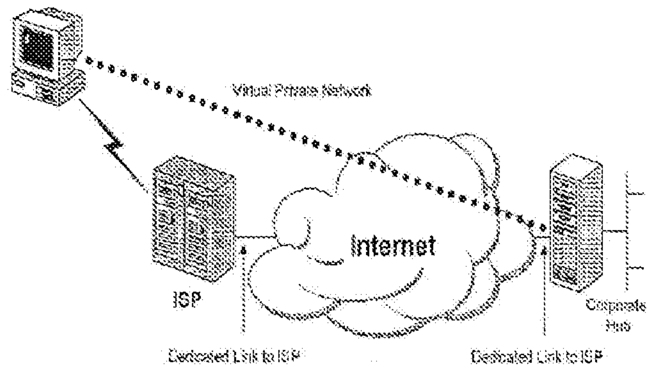


Figure 2: Using a VPN to connect a remote client to a private LAN

To this end, according to page 8 of VPN Overview, a user calls a local ISP and using the connection to the local ISP, the VPN software creates a virtual private network between the dial-up user and the corporate VPN server across the Internet.

31. VPN Overview provides no indication that the client is sending a domain name to the Front End Processor ("FEP") to establish a connection; instead, the indication is that the client is establishing a dial-up connection to the FEP. At page 22, VPN Overview states "[i]n the Internet example, the client computer places a dial-up call to a tunneling-enabled NAS at the ISP." Even assuming for the sake of argument that the alleged domain name is sent from the client to the FEP, the VPN Overview provides no evidence that the alleged domain name is a <u>secure</u> domain name in the context of this application. As I stated in ¶¶ 9-12, a <u>secure</u> domain name, as recited in claims 1, 17, and 33 of the '180 Patent, is not a domain name that just happens to be associated with a computer used to establish a secure connection. The Request also alleges that VPN Overview describes a secure domain name because the domain name for the VPN tunnel server happens to correspond to a network address allegedly requiring authentication. As I stated in ¶¶ 9-12, however, a <u>secure</u> domain name is not a domain name that so happens to correspond to a network address for a server involved in securing communications.

32. The domain name of the VPN tunnel server is also not a <u>secure</u> domain name, even if this recitation is incorrectly defined according to the Request. The Request asserts that a secure domain name corresponds to a secure computer network address. However, the address of the VPN tunnel server is not a secure computer network address, for the reasons I stated in ¶ 11. Assuming for the sake of argument that the Request correctly interprets a <u>secure</u> computer network address to be associated with a computer which requires authorization for access, then, without authorization for access, a client computer cannot communicate with a secure computer network address. In VPN Overview, however, a client computer may communicate with a VPN tunnel server without pre-authorization to access the hosts protected by the VPN tunnel server. Thus, because the VPN tunnel server of the reference does not require authorization for access, it is not associated with a <u>secure</u> computer network address, and therefore also cannot be associated with a secure domain name.

33. VPN Overview also has not been shown to teach a secure domain name service. VPN Overview, on page 26, describes that redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common

security perimeter. The round-robin DNS, however, is no different from a conventional DNS. As I stated in ¶¶ 9-12, however, a secure domain name service is not a conventional DNS. Specifically, a secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name.

34. The proposed combination of VPN Overview and RFC 1035 has not been shown to describe or suggest a secure domain name and a secure domain name service as recited in claims 1, 17, and 33. RFC 1035, at page 4, describes user programs that interact with the domain name space through resolvers; the format of user queries and user responses is specific to the host and its operating system. User queries will typically be operating system calls, and the resolver and its cache will be part of the host operating system. Resolvers answer user queries with information they acquire via queries to foreign name servers and the local cache.

35. Even assuming for the sake of the argument that this description supports the allegation that the user query corresponds to a domain name and the resolver corresponds to a domain name service, RFC 1035 still fails to describe or suggest a secure domain name and a secure domain name service, as I outlined in ¶¶ 9-12 above. RFC 1035 is not seen to show anything other than a conventional DNS.

36. The Request also points to no evidence that distinguishes the alleged DNS of RFC 1035 from a conventional DNS. Instead, the Request merely states that RFC 1035, on page 22, discloses that the domain name is sent to a domain name service for resolution and then passed back the IP address. As stated above in ¶¶ 9-12, a secure domain name service is unlike a conventional DNS. Specifically, a secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name. As such, the proposed addition of subject matter from RFC 1035 fails to remedy the shortcomings of VPN Overview to describe or suggest a secure domain name or secure domain name service, as recited in claims 1, 17, and 33.

37. Furthermore, the proposed combination of the VPN Overview and RFC 1035 also fails to describe or suggest a secure domain name or a secure domain name service even if these recitations are incorrectly defined as suggested by the Request. The Request, at pages 21-22, asserts that the secure domain name corresponds to a secure computer network address, and a secure domain name service corresponds to a lookup service that returns a secure network address for the requested secure domain name. The proposed combination of the VPN Overview and RFC 1035, in fact, does not teach these features.

38. The proposed combination of the VPN Overview and RFC 1035, at best, shows a DNS server that can allegedly receive the domain name of the VPN tunnel server and can allegedly resolve and return the IP address for the domain name of the VPN tunnel server. As noted above, the issue is that the purpose of the VPN tunnel server is to secure a connection to resources behind the VPN tunnel server. To this end, for the reasons I stated in ¶ 11, the VPN tunnel server itself is not secure – that is, it does not require authorization for access. Therefore, neither the domain name of the VPN tunnel server nor its corresponding computer network address is secure – even if this term is defined as proposed by the Request.

39. As such, even under the Request's incorrect claim interpretation, the proposed combination of the VPN Overview and RFC 1035 has not been shown to describe or suggest a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33.

The Kosiur Reference

40. Kosiur has not been shown to describe or suggest a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33. At pages 295-96, Kosiur describes protecting external access to a company's intranet by establishing two corporate DNS servers: one external to the firewall and one internal. The external corporate DNS includes a list of hosts that the company permits the public to access, such as, for example, the company's e-mail gateway, public web site, and anonymous FTP server. The internal corporate DNS includes a list of hosts that only the company's internal network users are permitted to access. When an internal host attempts to access an external host, the internal DNS server forwards the DNS request to the external DNS server. In the reverse, however, if an external host attempts to access an internal host, then the external host must connect to the internal DNS server through a VPN.

41. Although Kosiur describes a domain name, it does not describe a secure domain name, as recited in claims 1, 17, and 33. The Request asserts that Kosiur discloses "domain name usage with VPN enabled servers and computers." These domain names, the Request asserts, are "secure" because the domain names correspond to a network address that requires authentication. This is incorrect. Such a reading of a claim is contrary to its meaning and reads out a critical aspect of the invention. For the reasons I stated in ¶¶ 9-12, a secure domain name is not a domain name that just happens to correspond to a network address that requires authentication.

42. Kosiur has also not been shown to disclose a secure domain name service, as recited in claims 1, 17, and 33. The Request alleges that a secure domain name service is a look-up request to a domain name service to resolve a domain name identifying VPN resources. Kosiur describes an internal DNS and an external DNS for resolving addresses of internal hosts and external hosts respectively. Kosiur has not been shown to disclose that either the internal or external DNS is different from a conventional DNS. Further, the Request provides no evidence that the DNS disclosed by Kosiur is different from a conventional DNS. The Request, at page 28 simply states that "Kosiur discloses at pages 293-296 that domain name resolution occurs at DNS servers. The DNS servers pass back the corresponding network address." Thus, Kosiur has not been shown to disclose anything other than a conventional DNS, and, as I stated in ¶¶ 9-12, a secure domain name service is not a conventional domain name service. Specifically, a secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name.

43. As such, Kosiur has not been shown to teach a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33.

The Kaufman Reference

44. At page 2, Kaufman discloses the use of IPsec to secure communications through the Internet using authentication and encryption. At page 128, Kaufman also describes a domain name service being an integral part of the Internet and of any normal IP network. At page 243, the domain name service is described as a protocol used to support hierarchical resolution of host names to IP addresses (and vice versa) in the Internet. Kaufman also describes that a layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network. The Request alleges that an IPsec connection request over the Internet for a secured resource can use, for example, a DNS server to resolve the request. Even assuming, *arguendo*, this assertion is correct, it falls short of describing a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33.

45. Kaufman has not been shown to teach or disclose a secure domain name, as recited in claims 1, 17, and 33. Similar to previous assertions, the Request suggests that Kaufman describes a secure domain name simply because it describes a domain name corresponding to a network address involving security (*e.g.* a computer protected by a home network). As I stated in ¶¶ 9-12, however, a secure domain name cannot be properly read to be a domain name that just happens to be associated with a computer network address requiring authentication because this interpretation is inconsistent with the meaning adopted by the inventors of the ‘180 Patent.

46. Kaufman also has not been shown to describe or suggest a secure domain name service, as recited in claims 1, 17, and 33. The Request, at page 32, alleges that a “‘secure domain name service’ includes any lookup service that resolves a secure domain name.” Assuming, for the sake of argument, that Kaufman discloses a secure domain name, Kaufman has not been shown to disclose a secure domain name service because it has only been shown to disclose a conventional DNS. As I provided in ¶¶ 9-12, a secure domain name service is unlike a conventional DNS. Specifically, a secure domain name service is not a conventional DNS that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be requesting resolution of a secure domain name.

47. The Request also seems to allege that Kaufman’s disclosure of DNS Security (“DNSSEC”) is a secure domain name service. To the extent Kaufman even discloses DNSSEC, that protocol merely teaches protecting the integrity of the traditional DNS resolution process. This “conventional scheme” of protecting the integrity of DNS resolution is also explicitly disclosed in column 40, lines 6-14 of the specification of the ‘180 Patent as being conventional:

> One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project (RFC 2535).

As I noted above, the inventors had explicitly contemplated this "conventional scheme" of performing DNS resolution, and nevertheless claimed a secure domain name service as being something different. The addition of security to protect the integrity of a traditional DNS look-up does not teach a secure domain name service for the same reasons as I identified in ¶¶ 9-12.

48. Kaufman has not been shown to describe or suggest a secure domain name or a secure domain name service as recited in claims 1, 17, and 33.

The Kaufman and Galvin References

49. I incorporate here my statements made immediately above in ¶¶ 42-46 regarding Kaufman.

50. According to page 38 of the Request, Galvin is cited to teach "a second type of 'secure domain name service' that includes digitally signed resource records." Galvin at §§ 1 and 3.2 discloses using a public key in the DNS resolution process to protect the integrity of the process. This "conventional scheme" protecting the integrity of DNS resolution is also explicitly disclosed in column 40, lines 6-14 of the specification of the '180 Patent:

> One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project (RFC 2535).

Thus, the inventors had explicitly contemplated this "conventional scheme" of performing DNS resolution, and nevertheless claimed a secure domain name service as being something different.

51. This aspect of Galvin does not teach the secure domain name service recited in claims 1, 17, and 33. The Request assumes that a "secure domain name service" is a conventional domain name service which issues a public key to ensure that the service is trustworthy. As I stated above, however, in ¶¶ 9-12, disclosure of a conventional domain name service does not disclose a secure domain name service. The addition of a public key to ensure the integrity of a DNS look-up does not teach a secure domain name service. As such, Galvin fails to remedy the shortcomings of Kaufman to describe or suggest a secure domain name service as recited in claims 1, 17, and 33.

The Gauntlet Reference

52. According to Gauntlet at page 1-1, "[a] firewall is a single point of defense that protects one side from the other. In networking situations, this usually means protecting a company's private network from other networks to which it is connected." Gauntlet teaches a system that prohibits all network traffic through the firewall unless it is "expressly permitted."

53. The disclosed firewall operates as follows, as described on pages 1-6 to 1-8. The firewall necessarily must see the network traffic communicating with the protected side of the wall, *i.e.*, the private network. After receiving a packet, the firewall checks the source and destination address of the packet against its user-defined rules, and then checks the type of request sought. If the requested service is supported and authorized, the appropriate program is called and the request is processed.

54. According to pages 5-1 to 5-2, when determining if access should be permitted or denied, the firewall checks the IP address provided in the packet request against the user-provided rules. The rules can be defined by hostname or by IP address. Because the received packet identifies sources and destinations by IP addresses, if the rule is defined by hostname, additional steps are taken to convert an IP address identified in the packet to a hostname. In other words, "the proxy must use DNS to map the source or destination address (in the packet) into a host name" – the proxy performs a reverse DNS lookup.

55. According to chapter 18 of Gauntlet, the Gauntlet firewall also offers Point-to-Point Tunneling Protocol ("PPTP") services to permit clients on an untrusted network to establish connection to a PPTP server on the protected network. To allow PPTP connections, however, the administrator of the firewall "must advertise the IP address of the PPTP server" and users "must connect directly to the server IP address." To "advertise" an IP address, as used in Gauntlet, merely requires that the IP address be accessible to the public.

56. The Request alleges that, since PPTP connections can be identified using domain names, where a domain name corresponds to a PPTP enabled server, its domain name is a <u>secure</u> domain name. As I stated in ¶¶ 9-12, a <u>secure</u> domain name cannot be properly read to be a domain name that just happens to be associated with a server which is used to establish PPTP connections between a client and a target.

57. Similarly, to the extent that Gauntlet describes a conventional DNS, a <u>secure</u> domain name service cannot be properly read to be a conventional DNS. The Request alleges that, since PPTP connections can be identified using domain names, where a domain name corresponds to a PPTP enabled server, its domain name is a secure domain name, and the resolution of that domain name into a network address occurs at a secure domain name service. First, Gauntlet discloses at 18-1 that the administrator of the firewall "must advertise the IP address of the PPTP server" and users "must connect directly to the server IP address." Gauntlet has not been shown to disclose a DNS resolution for a hostname for a PPTP server. Second, to the extent that Gauntlet describes a DNS, it describes a conventional DNS and not a <u>secure</u> DNS. As noted at the outset of Section I.C., a <u>secure</u> domain name service differs from a conventional DNS, as I demonstrated in ¶¶ 9-12.

58. The Request also alleges that the use of a PPTP service, offered by the Gauntlet firewall software, requires the use of a PPTP server whose network address is a <u>secure</u> computer network address. The Gauntlet firewall offers PPTP services to permit clients on an untrusted network to establish connection to a PPTP server on the protected network. The network address of a PPTP server, however, is not a <u>secure</u> computer network address because it does not require authorization for access, as I stated above in ¶ 11. That is, a client can communicate with the PPTP server without authorization.

<u>The Hands-On and Installing NT References</u>

59. Installing NT is a white paper on the PPTP network protocol. According to pages 20-22, Installing NT discloses the creation of a phonebook entry to dial a PPTP server. The Request refers to Figure 12 in that reference to disclose a domain name for a PPTP server; the Figure is reproduced below:

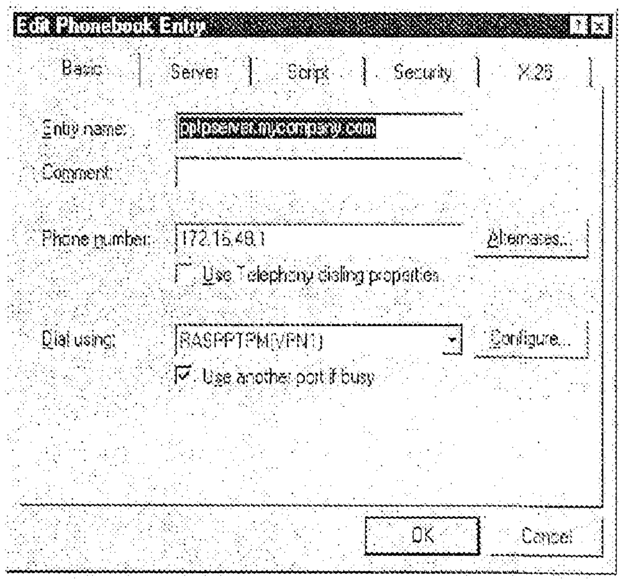


Figure 12 – Example Phonebook entry for PPTP server and a VPN device

The Request, at pages 47-48, refers to this figure to state that "PPTP connections can be identified using domain names" by indicating that the "Entry name" in the Figure is the domain name. This is incorrect. The "Entry name" is simply an arbitrary name to identify the Phonebook entry. It does not *correspond* to a domain name of a PPTP server that would be resolved to via a "traditional DNS server" to the network address of the PPTP server, as asserted on page 48 of the Request.

60. Hands-On is a technical and training manual for Microsoft Windows NT. The Request describes Hands-On as disclosing PPTP, traditional DNS according to RFC 1035, and an AutoDial feature, which I describe below.

61. The Request alleges that Installing NT teaches that a name for a PPTP server is a "secure domain name." The Request, at page 47, asserts that a PPTP server's network address is a secure network address and that identifying the PPTP server with a domain name teaches a "secure domain name." To the contrary, such an arbitrary identification is not a <u>secure</u> domain name. As I demonstrated above in ¶¶ 9-12, a <u>secure</u> domain name cannot be properly read to be a domain name that just happens to be associated with a server which is used to establish PPTP connections between a client and a target. Neither the Office Action nor the Request demonstrate any aspect of Installing NT that teaches or discloses anything other than a domain name that just happens to be associated with a PPTP server.

62. Hands-On similarly has not been shown to describe this feature. Notably, the Request does not rely on this reference to show this feature. Nevertheless, for the reasons I stated in ¶¶ 9-

12, to the extent that Hands-On discloses domain names, such a disclosure does not teach or disclose a secure domain name, as recited in claims 1,17, and 33.

63. The Request also alleges that Hands-On discloses a secure domain name service. The Request asserts that Hands-On discloses two "lookup services" that allegedly disclose the secure domain name service recited in claims 1, 17, and 33. The first one is a "traditional DNS server." According to the Request, sending a query message to a traditional DNS to resolve the domain name of the PPTP server disclosed in Installing NT (and described above) renders the traditional DNS a secure domain name service. As I stated previously at ¶¶ 9-12, a conventional DNS is not transformed into a secure domain name service by merely resolving a query, that, unbeknownst to the secure domain name service, is requesting the address of a PPTP server.

64. The second "look-up service" disclosed in Hands-On also does not disclose the secure domain name service of claims 1, 17, and 33. This "alternative 'lookup service'" is called AutoDial. According to Hands-On at 462, AutoDial "maps and maintains network addresses to phonebook entries" such that, when an application or command requests access to an IP address, the client computer will match that network address to the phonebook entry and dial the phone number associated with that network address. Although an AutoDial database can include IP addresses and Internet host names, these addresses are each associated with a phonebook entry, which provides a phone number to be dialed for connecting with said IP addresses and Internet host names. Thus, AutoDial is not disclosed to resolve domain names to IP addresses, much less to resolve a secure domain name into a secure computer network address. Nevertheless, even assuming for the sake of argument that AutoDial were shown to teach a conventional DNS, a conventional DNS does not teach a secure domain name service, as I described in ¶¶ 9-12 above.

65. The Request also alleges that, because a PPTP server, which enables a PPTP connection between a client and a target, may be referenced by a domain name, its domain name is a "secure domain name" and its network address is a "secure computer network address." The network address for a PPTP server is not a secure network address because a client can communicate with the PPTP server without authorization, as I stated above in ¶ 11.

The Microsoft VPN Reference

66. Microsoft VPN is a compilation of various Microsoft documents. As identified by the Request at page 52, Microsoft VPN discloses PPTP connections for remote users to access a corporate network. Microsoft VPN discloses at page 32, creating an IP address or host name of a corporate office "VPN" server. Microsoft VPN Microsoft VPN also discloses a conventional DNS structure at pages 64-66. Microsoft VPN, however, has not been shown to teach or disclose a secure domain name or a secure domain name service, as recited in claims 1, 17, and 33.

67. The Request asserts that the hostname associated with a PPTP server, which is used to establish PPTP connections between a client and a target computer is a secure domain name. This is incorrect. A secure domain name cannot be properly read to be a domain name that just happens to be associated with a server which is used to establish PPTP connections between a client and target, as I stated above in ¶¶ 9-12.

68. The Request, at page 54, also alleges that, since Microsoft VPN discloses a conventional DNS, which resolves domain names, a DNS request for the IP address for a PPTP server renders the traditional DNS a secure domain name service. A conventional DNS is not transformed into a secure domain name service merely by resolving a request for the IP address of a server which is used to establish PPTP connections. As I stated in ¶¶ 9-12, above, disclosure of a conventional DNS does not disclose a secure domain name service, as recited in claims 1, 17, and 33.

69. The Request, at page 54, also alleges that the network address of a PPTP server, which enables a PPTP connection between a client and a target, is a "secure computer network address." The network address for a PPTP server is not a secure network address because a client can communicate with the PPTP server without authorization, as I stated above in ¶ 11. Further, because it does not have a secure computer network address, its domain name cannot be secure domain name.

Truth and Accuracy of Statements

70. I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that willful false statements or the like may jeopardize the validity of the application or any patent issuing thereon.

Signed at New York, New York this 19 th day of April, 2010.

Jason Nieh, Ph.D.

BST99 1647647-6.077580.0090

EXHIBIT A

Jason Nieh - Curriculum Vitae

Columbia University	Office: (212) 939-7160
Department of Computer Science	Fax: (212) 666-0140
1214 Amsterdam Ave. MC0401	nieh@cs.columbia.edu
New York, NY 10027-7003	http://www.cs.columbia.edu/~nieh

RESEARCH INTERESTS

Mobile computing, operating systems, distributed systems, thin-client computing, web and multimedia systems, and performance evaluation.

EDUCATION

Ph.D. Electrical Engineering, **Stanford University**, Stanford, CA, June 1999. Dissertation: “The Design, Implementation, and Evaluation of SMART: A Scheduler for Multimedia Applications”, advisor Monica S. Lam.

M.S. Electrical Engineering, **Stanford University**, Stanford, CA, June 1990.

B.S. Electrical Engineering, **Massachusetts Institute of Technology**, Cambridge, MA, June 1989. Dissertation: “Using Special-Purpose Computing to Examine Chaotic Behavior in Nonlinear Mappings”, advisor Gerald J. Sussman.

HONORS

IBM Faculty Award, 2004, 2006, 2008.

LISA Best Student Paper Award, 2005.

Sigma Xi Young Investigator Award, 2004. Awarded biennially to one individual for scientific achievement in the physical sciences and engineering. First computer scientist to receive this national award.

ACM MobiCom Best Student Paper Award, 2004.

Distinguished Faculty Teaching Award, Columbia Engineering School Alumni Association, 2004. Awarded to the top two instructors in the School of Engineering and Applied Science at Columbia University.

IBM Shared University Research (SUR) Award, 2000, 2004.

IBM Performance Modeling and Analysis PIC Best Paper Award, 2004.

Department of Energy Early Career Principal Investigator Award, 2003.

National Science Foundation Faculty Early Career Development (CAREER) Award, 2001.

Sun Microsystems SAM Award, 1994.

GE Foundation Fellowship, 1989.

California Microelectronics Fellowship, 1989 (declined).

AT&T Engineering Scholarship, 1986-1989.

Member, Eta Kappa Nu, 1988.

Member, Sigma Xi, 1988.

Member, Tau Beta Pi, 1988.

PROFESSIONAL EXPERIENCE

Associate Professor of Computer Science, **Columbia University,** New York, NY, 2003 - present.

Director, Network Computing Laboratory, **Columbia University,** New York, NY, 2000 - present.

Founder, **Guitar Notes, Inc.**, New York, NY, 1996 - present.

Expert Witness, *01 Communique Laboratory v. Citrix Systems*, **Goodwin Procter**, Boston, MA, 2006 - 2008.

Chief Scientist, **DeskTone**, Chelmsford, MA, 2006 - 2007.

1st Scholar in Residence, **VMware**, Palo Alto, CA, 2006 - 2007.

Consultant, *Rothschild Trust v. Citrix Systems*, **Goodwin Procter**, Boston, MA, 2006.

Technical Advisor, *Microsoft Consent Decree*, **States of NY, OH, IL, KY, LA, MD, MI, NC, and WI**, 2003 - 2006.

Expert Witness, *Cox v. Microsoft*, **Milberg Weiss Bershad and Schulman,** New York, NY, 2005 - 2006.

Assistant Professor of Computer Science, **Columbia University,** New York, NY, 1999 - 2003.

Chairman of Technology Office and Director, **TrueMetrix,** New York, NY, 1999 - 2000.

Technical Consultant, **Vertex Management**, Redwood Shores, CA, 1996 - 1997.

Academic Consultant, **Sun Microsystems Laboratories**, Mountain View, CA, 1993 - 1998.

Research Assistant, Dept. of Electrical Engineering, **Stanford University**, Stanford, CA, 1990 - 1998.

Summer Institute in Parallel Computing, **Argonne National Laboratories**, Argonne, IL, 1991.

Undergraduate Researcher, **Massachusetts Institute of Technology**, Cambridge, MA, 1987 - 1989.

Summer Intern, **AT&T Bell Laboratories**, Lincroft, Middletown, and Murray Hill, NJ, 1986 - 1988.

RESEARCH SUPPORT (all co-principal investigators at Columbia University unless otherwise noted)

1. Principal Investigator, "TC:Small: Exploiting Software Elasticity for Automatic Software Self-Healing", Trustworthy Computing Program, **National Science Foundation**, CNS-0914845, $450,000, Sept. 1, 2009 - Aug. 31, 2012, with Angelos D. Keromytis.
2. Co-Principal Investigator, "CSR: Medium: Guanyin: a Thousand hands with a Thousand eyes for Distributed Software Checking", Computer Systems Research Program, **National Science Foundation**, CNS-0905246, $1,102,000, Sept. 1, 2009 - Aug. 31, 2013, with Junfeng Yang and Gail E. Kaiser.
3. Principal Investigator, "Google Desktop Meets DejaView: Display-Centric Desktop Search", Google Research Award, **Google**, $70,000, Sept. 1, 2009 - Aug. 31, 2010, with Luis Gravano.
4. Principal Investigator, "Android G1 Dev Phone Equipment Grant", **Google**, $23,940, Sept. 2009.
5. Principal Investigator, "DejaView / Android Development", Center for Advanced Technology in Telecommunications (CATT), **New York State Office of Science, Technology, and Academic Research (NYSTAR**), $20,000, Sept. 1, 2009 - Feb. 28, 2010.
6. Principal Investigator, "GOALI Supplement to CSR-VSM: Autonomic Mechanisms for Reducing System Downtime due to Maintenance and Upgrades", Grant Opportunities for Academic Liaison with Industry Program, **National Science Foundation**, CNS-0950434, $66,675, Sept. 1, 2009 - Aug. 31, 2010.
7. Principal Investigator, "CIFellow: Michael Hines", Subaward through Computing Community Consortium and Computing Research Association, **National Science Foundation**, CNS-0937060, $140,000, Sept. 1, 2009 - Aug. 31, 2010.
8. Principal Investigator, "An Open Standard for Advanced Display and Application Remoting", IBM Faculty Award, **IBM Research**, $20,000, July 1, 2008 - June 30, 2009.
9. Principal Investigator, "Remote 3D Gaming Research", **Deutsche Telekom AG, Laboratories**, $70,930, Sept. 1, 2007 - Aug. 31, 2008.
10. Principal Investigator, "Virtualization Mechanisms for Security", Center for Advanced Technology in Telecommunications (CATT), **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, $38,559, July 1, 2007 - June 30, 2008.
11. Principal Investigator, "Virtualization Curriculum Equipment Grant", **VMware**, $40,000, Sept. 2007.
12. Co-Principal Investigator, "CSR-VSM: Autonomic Mechanisms for Reducing System Downtime due to Maintenance and Upgrades", Computer Systems Research Program, **National Science Foundation**, CNS-0717544, $350,000, Aug. 1, 2007 - July 31, 2009, with Gail E. Kaiser.

13. Co-Principal Investigator, "Autonomic Recovery of Enterprise-Wide Systems After Attack or Failure with Forward Correction", Multidisciplinary University Research Initiative (MURI), **Air Force Office of Scientific Research (AFOSR)**, USAF/AFRL FA9550-07-1-0527, $4,826,940, May 1, 2007 - Apr. 30, 2012, with Anup K. Ghosh (George Mason University), Sushil Jajodia, (George Mason University), Angelos D. Keromytis, Salvatore J. Stolfo, and Peng Liu (Pennsylvania State University).
14. Principal Investigator, "Thin-Client Computing Research", **Advanced Micro Devices**, $50,000, Jan. 1, 2007 - Dec. 31, 2007.
15. Principal Investigator, "Secure Isolation Mechanisms for Untrusted Network Applications", Center for Advanced Technology in Telecommunications (CATT), **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, $10,000, July 1, 2006 - June 30, 2007.
16. Co-Principal Investigator, "Security Escorts For Not-Yet Trusted Software", Small Business Technology Transfer Research Program (STTR), **Office of the Secretary of Defense**, O064-SP2-1001, $99,981, Aug. 15, 2006 - May 15, 2007, with Charles Earl (Stottler Henke Associates).
17. Principal Investigator, "Virtualization Mechanisms for Security", Center for Advanced Technology in Telecommunications (CATT), **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, $38,559, July 1, 2006 - June 30, 2007.
18. Principal Investigator, "An Application Streaming Service for Ubiquitous Computing Access", IBM Faculty Award, **IBM Research**, $20,000, July 1, 2006 - June 30, 2007.
19. Principal Investigator, "BPC Supplement to ITR: Secure Remote Computing Services", Broadening Participation in Computing Program, **National Science Foundation**, CNS-0543869, $133,565, Sept. 15, 2005 - Sept. 14, 2007.
20. Principal Investigator, "US-Japan Cyber Trust Supplement to ITR: Secure Remote Computing Services", Cyber Trust Program, **National Science Foundation**, CNS-0535343, $77,280, July 1, 2005 - June 30, 2007.
21. Principal Investigator, "Secure Isolation Mechanisms for Untrusted Network Applications", Center for Advanced Technology in Telecommunications (CATT), **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, $12,500, July 1, 2005 - June 30, 2006.
22. Principal Investigator, "Sun Ray Software Performance", Collaborative Research Program, **Sun Microsystems**, $45,142, Feb. 2005.
23. Principal Investigator, "ITR: Secure Remote Computing Services", Information Technology Research (ITR) for National Priorities Program, **National Science Foundation**, CNS-0426623, $1,200,000, Sept. 15, 2004 - Aug. 31, 2009, with Gail E. Kaiser and Angelos D. Keromytis.
24. Principal Investigator, "Secure Isolation Mechanisms for Untrusted Network Applications", Center for Advanced Technology in Telecommunications (CATT), **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, $12,500, July 1, 2004 - June 30, 2005.
25. Principal Investigator, "Secure Isolation and Transparent Migration of Legacy Applications", IBM Faculty Award, **IBM Research**, $40,000, July 1, 2004 - June 30, 2005.
26. Principal Investigator, "Secure Isolation and Migration of Linux Applications", Center for Advanced Technology (CAT) in Information Management, **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, $70,000, Apr. 19, 2004 - June 30, 2004.
27. Principal Investigator, "Linux Virtualization Phase I", IBM Shared University Research (SUR) Award, **IBM Research**, $503,027, Mar. 2004.
28. Principal Investigator, "Migration Mechanisms for Large-Scale Parallel Applications", Early Career Principal Investigator Program in Applied Mathematics, Collaboratory Research, Computer Science, and High-Performance Networks, Office of Science, **US Department of Energy**, $299,589, Aug. 15, 2003 - Aug. 14, 2007.
29. Principal Investigator, "Sun Microsystems Equipment Grant", Collaborative Research Program, **Sun Microsystems**, $6,195, July 2003.
30. Principal Investigator, "Network Virtualization Mechanisms for Mobile Communication", Networking Research Program, **National Science Foundation**, ANI-0240525, $249,999, June 1, 2003 - May 31, 2007.

31. Principal Investigator, "Apple Computer Powerbook Award", Apple Developer Connection and Hardware Seed Program, **Apple Computer**, $7,433, May 2003.
32. Principal Investigator, "ITR: An Experimental Study of Thin-Client Computing Architectures", Information Technology Research (ITR) Program, **National Science Foundation**, CCR-0219943, $250,000, Sept. 1, 2002 - July 31, 2007.
33. Senior Personnel, "Pervasive Pixels", CISE Research Infrastructure Program, **National Science Foundation**, EIA-0202063, $1,485,098, Sept. 1, 2002 - Aug. 31, 2007, with Henning Schulzrinne, Steven K. Feiner, Gail E. Kaiser, John R. Kender, Kathleen R. McKeown, Peter K. Allen, Angelos D. Keromytis, Shree K. Nayar, William Noble, Steven M. Nowick, and Kenneth A. Ross.
34. Principal Investigator, "Migration Mechanisms for Autonomic Computing", Center for Advanced Technology (CAT) in Information Management, **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, $70,000, July 1, 2002 - June 30, 2003.
35. Principal Investigator, "Inferring Mean Client Response Time at the Web Server", Center for Advanced Technology (CAT) in Information Management, **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, $25,000, Apr. 1, 2002 - June 30, 2002.
36. Co-Principal Investigator, "The Columbia Hot Spot Rescue Service", Advanced Networking Infrastructure and Research (ANIR) Special Projects in Networking Program, **National Science Foundation**, ANI-0117738, $1,399,999, Sept. 15, 2001 - Aug. 30, 2006, with Edward G. Coffman, Predrag R. Jelenkovic, Dan Rubenstein, and Henning Schulzrinne.
37. Principal Investigator, "Scalability Issues in Linux", Collaborative Research Program, **IBM Linux Technology Center**, $33,029, July 1, 2001 - June 30, 2002.
38. Principal Investigator, "Thin-Client Benchmarking", **National Semiconductor**, $25,000, July 1, 2001 - June 30, 2002.
39. Principal Investigator, "Server-Based Computing Technologies for Application Service Providers", Center for Advanced Technology (CAT) in Information Management, **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, $75,000, July 1, 2001 - June 30, 2002.
40. Principal Investigator, "Scalable Linux Cluster Utilities", Center for Advanced Technology (CAT) in Information Management, **New York State Office of Science, Technology, and Academic Research (NYSTAR)**, $50,000, Apr. 16, 2001 - June 30, 2001.
41. Principal Investigator, "CAREER: Delivering Computational Services over the Internet", Faculty Early Career Development (CAREER) Award, Operating Systems and Compilers Program, **National Science Foundation**, CCR-0093047, $250,000, Feb. 15, 2001 - Feb. 28, 2007.
42. Principal Investigator, "Scalable Linux Cluster Computer Utilities", IBM Shared University Research (SUR) Award, **IBM Research**, $128,162, Dec. 2000.
43. Co-Principal Investigator, "Adaptive Internet Interactive Team Video", Experimental Systems Program, **National Science Foundation**, EIA-0071954, $1,590,000, Sept. 15, 2000 - Sept. 30, 2004, with John R. Kender and Gail E. Kaiser.
44. Principal Investigator, "Columbia University Computer Utility", Collaborative Research Program, **Sun Microsystems**, $51,178, Sept. 1, 2000 - Oct. 31, 2001.
45. Principal Investigator, "Lucent Grant in Science and Engineering", University Program, **Lucent Technologies**, $20,000, July 2000.
46. Principal Investigator, "Sun Microsystems Equipment Grant", Collaborative Research Program, **Sun Microsystems**, $83,562, Dec. 1999.
47. Co-Principal Investigator, "Microsoft Research and Education Grant", Microsoft University Program, **Microsoft Research**, $1,208,163, July 1, 1999 - June 30, 2001, with Kathleen R. McKeown, Luis Gravano, John R. Kender, Andrew Kosoresow, Shree K. Nayar, and Henning Schulzrinne.

PUBLICATIONS

Most of these papers are available online at `http://www.ncl.cs.columbia.edu/publications`.

REFEREED JOURNAL ARTICLES

1. Albert M. Lai, Justin B. Starren, David R. Kaufman, Eneida A. Mendonca, Walter Palmas, Jason Nieh, and Steven Shea, "The Remote Patient Education in a Telemedicine Environment Architecture (REPETE)", *Telemedicine and e-Health*, 14(5), May 2008, pp. 355-361.
2. Albert Lai and Jason Nieh, "On the Performance of Wide-Area Thin-Client Computing", *ACM Transactions on Computer Systems (TOCS)*, 24(2), May 2006, pp. 175-209.
3. David P. Olshefski, Jason Nieh, and Dakshi Agarwal, "Using Certes to Infer Client Response Times at the Web Server", *ACM Transactions on Computer Systems (TOCS)*, 22(1), Feb. 2004, pp. 49-93. (2004 Best Paper, Performance Modeling and Analysis PIC, IBM Research; nominated for the 2004 Pat Goldberg Memorial Best Paper Awards in Computer Science, Electrical Engineering and Mathematics)
4. Jason Nieh and Monica S. Lam, "A SMART Scheduler for Multimedia Applications", *ACM Transactions on Computer Systems (TOCS)*, 21(2), May 2003, pp. 117-163.
5. Jason Nieh, S. Jae Yang, and Naomi Novik, "Measuring Thin-Client Performance Using Slow-Motion Benchmarking", *ACM Transactions on Computer Systems (TOCS)*, 21(1), Feb. 2003, pp. 87-115.

REFEREED CONFERENCE PAPERS

6. Shaya Potter and Jason Nieh, "Apiary: Easy-to-use Desktop Application Fault Containment on Commodity Operating Systems", *Proceedings of the 2010 USENIX Annual Technical Conference (USENIX 2010)*, Boston, MA, June 23-25, 2010. (17% accepted, 24/141)
7. Oren Laadan, Nicolas Viennot, and Jason Nieh, "Transparent, Lightweight Application Execution Replay on Commodity Multiprocessor Operating Systems", *Proceedings of the ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2010)*, New York, NY, June 14-18, 2010. (16% accepted, 29/184)
8. Haoqiang Zheng and Jason Nieh, "RSIO: Automatic User Interaction Detection and Scheduling", *Proceedings of the ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2010)*, New York, NY, June 14-18, 2010. (16% accepted, 29/184)
9. Oren Laadan, Dan Phung, and Jason Nieh, "Operating System Virtualization: Practice and Experience", *Proceedings of the 3rd Annual Haifa Experimental Systems Conference (SYSTOR 2010)*, Haifa, Israel, May 24-26, 2010. (58% accepted, 18/31)
10. Oren Laadan, Jason Nieh, and Nicolas Viennot, "Teaching Operating Systems Using Virtual Appliances and Distributed Version Control", *Proceedings of the 41st ACM Technical Symposium on Computer Science Education (SIGCSE 2010)*, Milwaukee, WI, Mar. 10-13, 2010, pp. 480-484. (34% accepted, 103/303)
11. Shaya Potter, Ricardo Baratto, Oren Laadan, Leonard Kim, and Jason Nieh, "MediaPod: A Personalized Multimedia Desktop In Your Pocket", *Proceedings of the 11th IEEE International Symposium on Multimedia (ISM 2009)*, San Diego, CA, Dec. 14-16, 2009, pp. 219-226. (20% accepted, 30/153)
12. Alex Sherman, Jason Nieh, and Clifford Stein, "FairTorrent: Bringing Fairness to Peer-to-Peer Systems", *Proceedings of the 5th ACM Conference on emerging Networking EXperiments and Technologies (CoNEXT 2009)*, Rome, Italy, Dec. 1-4, 2009, pp. 133-144. (17% accepted, 29/170, one of the top three papers submitted, fast tracked to *IEEE/ACM Transactions on Networking*)
13. Shaya Potter, Steven M. Bellovin, and Jason Nieh, "Two-Person Control Administration: Preventing Administration Faults Through Duplication", *Proceedings of the 23rd Large Installation System Administration Conference (LISA 2009)*, Baltimore, MD, Nov. 1-6, 2009, pp. 15-27. (32% accepted, 12/38)
14. Shaya Potter, Ricardo Baratto, Oren Laadan, and Jason Nieh, "GamePod: Persistent Gaming Sessions on Pocketable Storage Devices", *Proceedings of the 3rd International Conference on Mobile Ubiquitous Computing, Systems, Services, and Technologies (UBICOMM 2009)*, Sliema, Malta, Oct. 11-16, 2009. (32% accepted)

15. Angelos Stavrou, Ricardo Baratto, Angelos Keromytis, and Jason Nieh, "A2M: Access-Assured Mobile Desktop Computing", *Proceedings of the 12th Information Security Conference (ISC 2009)*, Pisa, Italy, Sept. 7-9, 2009, pp. 186-201. (28% accepted, 29/105)
16. Alex Sherman, Angelos Stavrou, Jason Nieh, Angelos Keromytis, and Clifford Stein, "Adding Trust to P2P Distribution of Paid Content", *Proceedings of the 12th Information Security Conference (ISC 2009)*, Pisa, Italy, Sept. 7-9, 2009, pp. 459-474. (28% accepted, 29/105)
17. Haoqiang Zheng and Jason Nieh, "WARP: Enabling Fast CPU Scheduler Development and Evaluation", *Proceedings of the 2009 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS 2009)*, Boston, MA, Apr. 19-21, 2009, pp. 101-112. (28% accepted, 24/86)
18. Stelios Sidiroglou, Oren Laadan, Carlos R. Pérez, Nicolas Viennot, Jason Nieh, and Angelos D. Keromytis, "ASSURE: Automatic Software Self-healing Using REscue points", *Proceedings of the 14th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2009)*, Washington, DC, Mar. 7-11, 2009, pp. 37-48. (26% accepted, 29/113)
19. Shaya Potter, Jason Nieh, and Matthew Selsky, "Secure Isolation of Untrusted Legacy Applications", *Proceedings of the 21st Large Installation System Administration Conference (LISA 2007)*, Dallas, TX, Nov. 11-16, 2007, pp. 117-130. (40% accepted, 22/55)
20. Albert Lai, Jason Nieh, and Justin Starren, "REPETE2: A Next Generation Home Telemedicine Architecture", *Proceedings of the American Medical Informatics Association (AMIA) 2007 Annual Symposium*, Chicago, IL, Nov. 10-14, 2007, p. 1020. (poster paper)
21. Oren Laadan, Ricardo Baratto, Shaya Potter, Dan Phung, and Jason Nieh, "DejaView: A Personal Virtual Computer Recorder", *Proceedings of the 21st ACM Symposium on Operating Systems Principles (SOSP 2007)*, Stevenson, WA, Oct. 14-17, 2007. pp. 279-292. (19% accepted, 25/130)
22. Oren Laadan and Jason Nieh, "Transparent Checkpoint/Restart of Multiple Processes on Commodity Operating Systems", *Proceedings of the 2007 USENIX Annual Technical Conference (USENIX 2007)*, Santa Clara, CA, June 17-22, 2007, pp. 323-336. (21% accepted, 24/117)
23. Stelios Sidiroglou, Oren Laadan, Angelos D. Keromytis, and Jason Nieh, "Using Rescue Points to Navigate Software Recovery (Short Paper)", *Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP 2007)*, Oakland, CA, May 20-23, 2007, pp. 273-280. (short paper, 12% accepted, 28/243, 8 short papers, 20 full papers)
24. Joeng Kim, Ricardo Baratto, and Jason Nieh, "An Application Streaming Service for Mobile Handheld Devices", *Proceedings of the IEEE International Conference on Services Computing (SCC 2006)*, Chicago, IL, Sept. 18-22, 2006, pp. 323-326. (short paper, 13% accepted, 22 short papers, 29 full papers)
25. Shaya Potter and Jason Nieh, "Highly Reliable Mobile Desktop Computing in Your Pocket", *Proceedings of the IEEE Computer Society Signature Conference on Software Technology and Applications (COMPSAC 2006)*, Chicago, IL, Sept. 18-21, 2006, pp. 247-254. (29% accepted, 54/184)
26. Bogdan Caprita, Jason Nieh, and Clifford Stein, "Grouped Distributed Queues: Distributed Queue, Proportional Share Multiprocessor Scheduling", *Proceedings of the 25th Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC 2006)*, Denver, CO, July 23-26, 2006, pp. 72-81. (22% accepted, 30/136)
27. David P. Olshefski and Jason Nieh, "Understanding the Management of Client Perceived Pageview Response Time", *Proceedings of the Joint International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS/ Performance 2006)*, St. Malo, France, June 26-30, 2006, pp. 240-251. (14% accepted, 30/217)
28. Joeng Kim, Ricardo Baratto, and Jason Nieh, "pTHINC: A Thin-Client Architecture for Mobile Wireless Web", *Proceedings of the 15th International World Wide Web Conference (WWW2006)*, Edinburgh, Scotland, May 23-26, 2006, pp. 143-152. (10% accepted, 70/673)
29. Shaya Potter and Jason Nieh, "Reducing Downtime Due to System Maintenance and Upgrades", *Proceedings of the 19th Large Installation System Administration Conference (LISA 2005)*, San Diego, CA, Dec. 4-9, 2005, pp. 47-62. (46% accepted, 24/52, Best Student Paper Award)
30. Bogdan Caprita, Jason Nieh, and Wong Chun Chan, "Group Round Robin: Improving the Fairness and Complexity of Packet Scheduling", *Proceedings of the 1st ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS 2005)*, Princeton, NJ, Oct. 26-28, 2005, pp. 29-40. (32% accepted, 23/71)

31. Ricardo Baratto, Leonard Kim, and Jason Nieh, "THINC: A Virtual Display Architecture for Thin-Client Computing", *Proceedings of the 20th ACM Symposium on Operating Systems Principles (SOSP 2005)*, Brighton, United Kingdom, Oct. 23-26, 2005, pp. 277-290. (13% accepted, 20/155)
32. Oren Laadan, Dan Phung, and Jason Nieh, "Transparent Checkpoint-Restart of Distributed Applications on Commodity Clusters", *Proceedings of the 2005 IEEE International Conference on Cluster Computing (Cluster 2005)*, Boston, MA, Sept. 27-30, 2005, 13 pages. (35% accepted, 45/130)
33. Shaya Potter and Jason Nieh, "AutoPod: Unscheduled System Updates with Zero Data Loss", *Proceedings of the 2nd IEEE International Conference on Autonomic Computing (ICAC 2005)*, Seattle, WA, June 13-16, 2005, pp. 367-368. (poster paper, 38% accepted, 64/170, 39 poster papers, 25 full papers)
34. Shaya Potter and Jason Nieh, "WebPod: Persistent Web Browsing Sessions with Pocketable Storage Devices", *Proceedings of the 14th International World Wide Web Conference (WWW2005)*, Chiba, Japan, May 10-14, 2005, pp. 603-612. (14% accepted, 77/550, nominated for Best Presentation Award)
35. Bogdan Caprita, Wong Chun Chan, Jason Nieh, Clifford Stein, and Haoqiang Zheng, "Group Ratio Round Robin: O(1) Proportional Share Scheduling for Uniprocessor and Multiprocessor Systems", *Proceedings of the 2005 USENIX Annual Technical Conference (USENIX 2005)*, Anaheim, CA, Apr. 10-15, 2005, pp. 337-352. (20% accepted, 24/118)
36. Jason Nieh and Chris Vaill, "Experiences Teaching Operating Systems Using Virtual Platforms and Linux", *Proceedings of the 36th ACM Technical Symposium on Computer Science Education (SIGCSE 2005)*, St. Louis, MO, Feb. 23-27, 2005, pp. 520-524. (32% accepted, 104/330)
37. Angelos Stavrou, Angelos D. Keromytis, Jason Nieh, Vishal Misra, and Dan Rubenstein, "MOVE: An End-to-End Solution To Network Denial of Service", *Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS 2005)*, San Diego, CA, Feb. 2-4, 2005, pp. 81-96. (13% accepted, 16/124)
38. David P. Olshefski, Jason Nieh, and Erich Nahum, "ksniffer: Determining the Remote Client Perceived Response Time from Live Packet Streams", *Proceedings of the 6th Symposium on Operating System Design and Implementation (OSDI 2004)*, San Francisco, CA, Dec. 6-8, 2004, pp. 333-346. (14% accepted, 27/193)
39. Ricardo Baratto, Shaya Potter, Gong Su, and Jason Nieh, "MobiDesk: Mobile Virtual Desktop Computing", *Proceedings of the 10th International Conference on Mobile Computing and Networking (MobiCom 2004)*, Philadelphia, PA, Sept. 29-Oct. 1, 2004, pp. 1-15. (8% accepted, 26/327, Best Student Paper Award)
40. Albert Lai, Jason Nieh, Andrew Laine, and Justin Starren, "Remote Display Performance for Wireless Healthcare Computing", *Proceedings of the 11th World Conference on Medical Informatics (Medinfo 2004)*, San Francisco, CA, Sept. 7-11, 2004, pp. 1438-1442. (42% accepted, 300/711)
41. Albert Lai, Jason Nieh, Bhagyashree Bohra, Vijayarka Nandikonda, Abhishek P. Surana, and Suchita Varshneya, "Improving Web Browsing on Wireless PDAs Using Thin-Client Computing", *Proceedings of the 13th International World Wide Web Conference (WWW2004)*, New York, NY, May 17-22, 2004, pp. 143-154. (15% accepted, 74/506)
42. Erez Zadok, Jeffrey Osborn, Ariye Shater, Charles Wright, Kiran-Kumar Muniswamy-Reddy, and Jason Nieh, "Reducing Storage Management Costs via Informed User-Based Policies", *Proceedings of the 12th NASA / Twenty-first IEEE Conference on Mass Storage Systems and Technologies (MSST)*, College Park, MD, Apr. 13-16, 2004, pp. 193-198. (short paper, 43% accepted, 32/75, 14 short papers, 18 full papers)
43. Haoqiang Zheng and Jason Nieh, "SWAP: A Scheduler with Automatic Process Dependency Detection", *Proceedings of the 1st USENIX/ACM Symposium on Networked Systems Design and Implementation (NSDI 2004)*, San Francisco, CA, Mar. 29-31, 2004, pp. 183-196. (< 23% accepted, 27/120+)
44. Albert Lai, Jason Nieh, Andrew Laine, and Justin Starren, "Thin Client Performance for Remote 3-D Image Display", *Proceedings of the American Medical Informatics Association (AMIA) 2003 Annual Symposium*, Washington, DC, Nov. 8-12, 2003, p. 904. (poster paper)
45. S. Jae Yang, Jason Nieh, Shilpa Krishnappa, Aparna Mohla, and Mahdi Sajjadpour, "Web Browsing Performance of Wireless Thin-Client Computing", *Proceedings of the 12th International World Wide Web Conference (WWW2003)*, Budapest, Hungary, May 20-24, 2003, pp. 68-79. (< 13% accepted, 77/600+)
46. Steven Osman, Dinesh Subhraveti, Gong Su, and Jason Nieh, "The Design and Implementation of Zap: A System for Migrating Computing Environments", *Proceedings of the 5th Symposium on Operating System Design and Implementation (OSDI 2002)*, Boston, MA, Dec. 9-11, 2002, pp. 361-376. (18% accepted, 27/150)

47. Albert Lai and Jason Nieh, "Limits of Wide-Area Thin-Client Computing", *Proceedings of the ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2002)*, Marina del Rey, CA, June 15-19, 2002, pp. 228-239. (13% accepted, 23/170)
48. David P. Olshefski, Jason Nieh, and Dakshi Agarwal, "Inferring Client Response Times at the Web Server", *Proceedings of the ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2002)*, Marina del Rey, CA, June 15-19, 2002, pp. 160-171. (13% accepted, 23/170)
49. S. Jae Yang, Jason Nieh, Matthew Selsky, and Nikhil Tiwari, "The Performance of Remote Display Mechanisms for Thin-Client Computing", *Proceedings of the 2002 USENIX Annual Technical Conference (USENIX 2002)*, Monterey, CA, June 10-15, 2002, pp. 131-146. (23% accepted, 25/107)
50. Fei Li and Jason Nieh, "Optimal Linear Interpolation Coding for Server-Based Computing", *Proceedings of the IEEE International Conference on Communications (ICC) 2002*, New York, NY, Apr. 28-May 2, 2002, pp. 2542-2546. (42% accepted, 655/1568)
51. Fei Li and Jason Nieh, "Low-complexity Interpolation Coding for Server-Based Computing", *Proceedings of the Data Compression Conference (DCC) 2002*, Snowbird, UT, Apr. 2-4, 2002, p. 461. (poster paper)
52. Jason Nieh, Chris Vaill, and Hua Zhong, "Virtual-Time Round-Robin: An O(1) Proportional Share Scheduler", *Proceedings of the 2001 USENIX Annual Technical Conference (USENIX 2001)*, Boston, MA, June 25-30, 2001, pp. 245-259. (29% accepted, 24/82, nominated for Best Paper Award)
53. S. Jae Yang, Jason Nieh, and Naomi Novik, "Measuring Thin-Client Performance Using Slow-Motion Benchmarking", *Proceedings of the 2001 USENIX Annual Technical Conference (USENIX 2001)*, Boston, MA, June 25-30, 2001, pp. 35-49. (29% accepted, 24/82)
54. Erez Zadok, Johan M. Andersen, Ion Badulescu, and Jason Nieh, "Fast Indexing: Support for Size-Changing Algorithms in Stackable File Systems", *Proceedings of the 2001 USENIX Annual Technical Conference (USENIX 2001)*, Boston, MA, June 25-30, 2001, pp. 289-304. (29% accepted, 24/82)
55. Erez Zadok and Jason Nieh, "FiST: A Language for Stackable File Systems", *Proceedings of the 2000 USENIX Annual Technical Conference (USENIX 2000)*, San Diego, CA, June 18-23, 2000, pp. 55-70. (30% accepted; 27/90)
56. Jason Nieh and Monica S. Lam, "The Design, Implementation and Evaluation of SMART: A Scheduler for Multimedia Applications", *Proceedings of the 16th ACM Symposium on Operating Systems Principles (SOSP 1997)*, St. Malo, France, Oct. 5-8, 1997, pp. 184-197. (< 20% accepted, 23/110+)
57. Jason Nieh and Monica S. Lam, "SMART UNIX SVR4 Support for Multimedia Applications", *Proceedings of the IEEE International Conference on Multimedia Computing and Systems (ICMCS 1997)*, Ottawa, Ontario, Canada, June 3-6, 1997, pp. 404-414. (~35% accepted)
58. Jason Nieh and Monica S. Lam, "SMART: A Processor Scheduler for Multimedia Applications", *Proceedings of the 15th Symposium on Operating Systems Principles (SOSP 1995)*, Copper Mountain Resort, CO, Dec. 3-5, 1995, p. 233. (poster paper, 40% accepted, 33/82, 11 poster papers, 22 full papers)

REFEREED WORKSHOP PUBLICATIONS

59. Alex Sherman, Jason Nieh, and Clifford Stein, "Fair Distributed Scheduling Algorithm for a P2P System", *9th Workshop on Models and Algorithms for Planning and Scheduling Problems (MAPSP 2009)*, Abbey Rolduc, The Netherlands, June 29-July 3, 2009.
60. Alfred Aho, Angelos D. Keromytis, Vishal Misra, Jason Nieh, Kenneth A. Ross, and Yechiam Yemini, "FlowPuter: A Cluster Architecture Unifying Switch, Server and Storage Processing", *Proceedings of the 1st International Workshop on Data Processing and Storage Networking: Towards Grid Computing (DPSN 2004)*, Athens, Greece, May 14, 2004, pp. 2/1-2/7 (60% accepted, 6/10).
61. Angelos D. Keromytis, Janak Parekh, Philip N. Gross, Gail Kaiser, Vishal Misra, Jason Nieh, Dan Rubenstein, and Sal Stolfo, "A Holistic Approach to Service Survivability", *Proceedings of the 2003 ACM Workshop on Survivable and Self-Regenerative Systems*, Fairfax, VA, Oct. 31, 2003, pp. 11-22. (38% accepted, 10/26)
62. Ed Coffman, Predrag Jelenkovic, Jason Nieh, Dan Rubenstein, and Henning Schulzrinne, "The Columbia Hotspot Rescue Service", *Internet2 Network Research Workshop Spring 2001*, Chicago, IL, Apr. 18-19, 2001.

63. Jason Nieh and S. Jae Yang, "Measuring the Multimedia Performance of Server-Based Computing", *Proceedings of the 10th Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV 2000)*, Chapel Hill, NC, June 26-28, 2000, pp. 55-64. (45% accepted, 32/70)
64. Jason Nieh and Monica S. Lam, "Multimedia on Multiprocessors: Where's the OS When You Really Need It?", *Proceedings of the 8th Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV 1998)*, Cambridge, UK, July 8-10, 1998, pp. 103-106. (45% accepted, 36/80)
65. Jason Nieh and Monica S. Lam, "Integrated Processor Scheduling for Multimedia", *Proceedings of the 5th Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV 1995)*, Durham, NH, Apr. 18-22, 1995, *Lecture Notes in Computer Science*, 1018, Springer-Verlag, pp. 215-218. (40% accepted, 40/101)
66. Jason Nieh, James G. Hanko, J. Duane Northcutt, and Gerard A. Wall, "SVR4 UNIX Scheduler Unacceptable for Multimedia Applications", *Proceedings of the 4th Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV 1993)*, Lancaster, United Kingdom, Nov. 3-5, 1993, *Lecture Notes in Computer Science*, 846, Springer-Verlag, pp. 35-48. (24% accepted, 24/100)
67. Jason Nieh and Marc Levoy, "Volume Rendering on Scalable Shared-Memory MIMD Architectures", *Proceedings of the Boston Workshop on Volume Visualization*, Boston, MA, Oct. 19-20, 1992, pp. 17-24.

INVITED BOOK CHAPTERS AND CONTRIBUTIONS

68. Albert Lai and Jason Nieh, "Web Content Delivery Using Thin-Client Computing", *Web Content Delivery*, ed. Samuel Chanson, Xueyan Tang, and Jianliang Xu, Springer, 2005, pp. 325-345.
69. Jason Nieh and Monica S. Lam, "The Design, Implementation and Evaluation of SMART: A Scheduler for Multimedia Applications", *Readings in Multimedia Computing and Networking*, ed. Kevin Jeffay and HongJiang Zhang, Morgan Kaufmann Publishers, 2002, pp. 506-519.

INVITED MAGAZINE ARTICLES

70. Shaya Potter and Jason Nieh, "Breaking the Ties that Bind: Process Isolation and Migration", *;login*, USENIX Association, 30(6), Dec. 2005, pp. 14-17.
71. S. Jae Yang and Jason Nieh, "MetaFrame XP Extends the Citrix Platform", *PC Magazine*, Ziff-Davis Media, 21(9), May 7, 2002, p. 48.
72. Jason Nieh and Ozgur C. Leonard, "Examining VMware", *Dr. Dobb's Journal*, 315, Miller Freeman, San Mateo, CA, Aug. 2000, pp. 70-76.
73. S. Jae Yang and Jason Nieh, "Thin Is In", *PC Magazine*, 19(13), Ziff-Davis Media, July 1, 2000, p. 68.

INVITED CONFERENCE PAPERS

74. Kenneth Ocheltree, Steven Millman, David Hobbs, Martin McDonnell, Jason Nieh, and Ricardo Baratto, "Net2Display: A Proposed VESA Standard for Remoting Displays and I/O Devices over Networks", *Proceedings of the 2006 Americas Display Engineering and Applications Conference (ADEAC 2006)*, Atlanta, Georgia, Oct. 23-26, 2006.

OTHER PUBLICATIONS

75. Dinesh Subhraveti and Jason Nieh, "Record and Transplay: Partial Checkpointing for Replay Debugging", Technical Report CUCS-050-09, Dept. of Computer Science, Columbia University, Nov. 2009.
76. Shaya Potter and Jason Nieh, "Apiary: Easy-to-use Desktop Application Fault Containment on Commodity Operating Systems", Technical Report CUCS-034-09, Dept. of Computer Science, Columbia University, Aug. 2009.
77. Alex Sherman and Jason Nieh, "FairStream: Improving Peer-to-Peer Streaming Performance through Fairness", Technical Report CUCS-018-09, Dept. of Computer Science, Columbia University, Apr. 2009.
78. Nicolas Viennot, Oren Laadan, and Jason Nieh, "Transparent, Lightweight Application Execution Replay on Commodity Multiprocessor Operating Systems", Technical Report CUCS-017-09, Dept. of Computer Science, Columbia University, Apr. 2009.
79. Alex Sherman, Jason Nieh, and Cliff Stein, "FairTorrent: Bringing Fairness to Peer-to-Peer Systems", Technical Report CUCS-011-09, Dept. of Computer Science, Columbia University, Mar. 2009.

80. Shaya Potter and Jason Nieh, “Improving Virtual Appliance Management through Virtual Layered File Systems”, Technical Report CUCS-008-08, Dept. of Computer Science, Columbia University, Jan. 2009.
81. Oren Laadan and Jason Nieh, “Operating System Virtualization: Practice and Experience”, Technical Report CUCS-058-08, Dept. of Computer Science, Columbia University, Dec. 2008.
82. Leon L. Wu, Gail E. Kaiser, Jason Nieh, and Christian Murphy, “Deux: Autonomic Testing System for Operating System Upgrades”, Technical Report CUCS-037-08, Dept. of Computer Science, Columbia University, Aug. 2008.
83. Alex Sherman, Jason Nieh, and Clifford Stein, “FairTorrent: Bringing Fairness to Peer-to-Peer Systems”, Technical Report CUCS-029-08, Dept. of Computer Science, Columbia University, May 2008.
84. Haoqiang Zheng and Jason Nieh, “Automatic User Interaction Detection and Scheduling with RSIO”, Technical Report CUCS-028-08, Dept. of Computer Science, Columbia University, May 2008.
85. Alex Sherman, Angelos Stavrou, Jason Nieh, and Clifford Stein, “Mitigating the Effect of Free-Riders in BitTorrent using Trusted Agents”, Technical Report CUCS-005-08, Dept. of Computer Science, Columbia University, Jan. 2008.
86. Alex Sherman, Angelos Stavrou, Jason Nieh, Clifford Stein, and Angelos D. Keromytis, “Can P2P Replace Direct Download for Content Distribution?”, Technical Report CUCS-020-07, Dept. of Computer Science, Columbia University, Mar. 2007.
87. Alex Sherman, Japinder Chawla, Jason Nieh, Clifford Stein, and Justin Sarma, “Aequitas: A Trusted P2P System for Paid Content Delivery”, Technical Report CUCS-019-07, Dept. of Computer Science, Columbia University, Mar. 2007.
88. Shaya Potter and Jason Nieh, “Improving Virtual Appliances through Virtual Layered File Systems”, Technical Report CUCS-003-07, Dept. of Computer Science, Columbia University, Jan. 2007.
89. Alex Sherman, Angelos Stavrou, Jason Nieh, Clifford Stein, and Angelos D. Keromytis, “A Case for P2P Delivery of Paid Content”, Technical Report CUCS-042-06, Dept. of Computer Science, Columbia University, Nov. 2006.
90. Alex Sherman, Jason Nieh, and Yoav Freund, “Feasibility of Voice over IP on the Internet”, Technical Report CUCS-027-06, Dept. of Computer Science, Columbia University, June 2006.
91. Jason Nieh and Chris Vaill, “Experiences Teaching Operating Systems Using Virtual Platforms and Linux”, *ACM Operating Systems Review (OSR)*, 40(2), Apr. 2006, pp. 100-104. (Reprint from *Proceedings of the 36th ACM Technical Symposium on Computer Science Education*, Feb. 2005.)
92. Bogdan Caprita, Jason Nieh, and Clifford Stein, “Grouped Distributed Queues: Distributed Queue, Proportional Share Multiprocessor Scheduling”, Technical Report CUCS-004-06, Dept. of Computer Science, Columbia University, Feb. 2006.
93. Jonathan Lennox, Henning Schulzrinne, Jason Nieh, and Ricardo A. Baratto, “Protocols for Application and Desktop Sharing”, Internet Draft draft-lennox-avt-app-sharing, IETF, Dec. 2004. Work in progress.
94. Henning Schulzrinne, Jonathan Lennox, Jason Nieh, and Ricardo A. Baratto, “Sharing and Remote Access to Applications”, Internet Draft draft-schulzrinne-mmusic-sharing, IETF, Sept. 2004. Work in progress.
95. Shaya Potter and Jason Nieh, “WebPod: Persistent Web Browsing Sessions with Pocketable Storage Devices”, Technical Report CUCS-047-04, Dept. of Computer Science, Columbia University, Nov. 2004.
96. Bogdan Caprita, Wong Chun Chan, Jason Nieh, Clifford Stein, and Haoqiang Zheng, “Group Ratio Round Robin: O(1) Proportional Share Scheduling for Uniprocessor and Multiprocessor Systems”, Technical Report CUCS-028-04, Dept. of Computer Science, Columbia University, July 2004.
97. Ricardo Baratto, Jason Nieh, and Leo Kim, “THINC: A Remote Display Architecture for Thin-Client Computing”, Technical Report CUCS-027-04, Dept. of Computer Science, Columbia University, July 2004.
98. Ricardo Baratto, Shaya Potter, Gong Su, and Jason Nieh, “MobiDesk: Mobile Virtual Desktop Computing”, Technical Report CUCS-014-04, Dept. of Computer Science, Columbia University, Mar. 2004.
99. Shaya Potter, Jason Nieh, and Dinesh Subhraveti, “Secure Isolation and Migration of Untrusted Legacy Applications”, Technical Report CUCS-005-04, Dept. of Computer Science, Columbia University, Jan. 2004.
100. Angelos D. Keromytis, Janak Parekh, Philip N. Gross, Gail Kaiser, Vishal Misra, Jason Nieh, Dan Rubenstein, and Sal Stolfo, “A Holistic Approach to Service Survivability”, Technical Report CUCS-021-03, Dept. of Computer Science, Columbia University, July 2003.

101. Bogdan Caprita, Wong Chun Chan, and Jason Nieh, "Group Round Robin: Improving the Fairness and Complexity of Packet Scheduling", Technical Report CUCS-018-03, Dept. of Computer Science, Columbia University, June 2003.
102. Wong Chun Chan and Jason Nieh, "Group Ratio Round-Robin: An O(1) Proportional Share Scheduler", Technical Report CUCS-012-03, Dept. of Computer Science, Columbia University, Apr. 2003.
103. Haoqiang Zheng and Jason Nieh, "SWAP: A Scheduler With Automatic Process Dependency Detection", Technical Report CUCS-005-03, Dept. of Computer Science, Columbia University, Apr. 2003.
104. Erez Zadok, Jeffrey Osborn, Ariye Shater, Charles Wright, Kiran-Kumar Muniswamy-Reddy, and Jason Nieh, "Reducing Storage Management Costs via Informed User-Based Policies", Technical Report FSL-03-01, Dept. of Computer Science, Stony Brook University, Mar. 2003.
105. Ozgur Can Leonard, Jason Nieh, Erez Zadok, Jeffrey Osborn, Ariye Shater, and Charles Wright, "The Design and Implementation of Elastic Quotas: A System for Flexible File System Management", Technical Report CUCS-014-02, Dept. of Computer Science, Columbia University, June 2002.
106. Ed Coffman, Predrag Jelenkovic, Jason Nieh, and Dan Rubenstein, "The Columbia Hot Spot Rescue Service: A Research Plan", Technical Report EE2002-005-131, Dept. of Electrical Engineering, Columbia University, May 2002.
107. Gong Su and Jason Nieh, "Mobile Communication with Virtual Network Address Translation", Technical Report CUCS-003-02, Dept. of Computer Science, Columbia University, Feb. 2002.
108. Hua Zhong and Jason Nieh, "CRAK: Linux Checkpoint / Restart As a Kernel Module", Technical Report CUCS-014-01, Dept. of Computer Science, Columbia University, Nov. 2001.
109. Erez Zadok, Johan M. Andersen, Ion Badulescu, and Jason Nieh, "Performance of Size-Changing Algorithms in Stackable File Systems", Technical Report CUCS-023-00, Dept. of Computer Science, Columbia University, Nov. 2000.
110. Jason Nieh, S. Jae Yang and Naomi Novik, "A Comparison of Thin-Client Computing Architectures", Technical Report CUCS-022-00, Dept. of Computer Science, Columbia University, Nov. 2000.
111. Erez Zadok and Jason Nieh, "FiST: A Language for Stackable File Systems", Technical Report CUCS-034-99, Dept. of Computer Science, Columbia University, Dec. 1999.
112. Jason Nieh, "The Design, Implementation, and Evaluation of SMART: A Scheduler for Multimedia Applications", Ph.D. Thesis, Dept. of Electrical Engineering, Stanford University, June 1999.
113. Jason Nieh and Monica S. Lam, "The Design, Implementation and Evaluation of SMART: A Scheduler for Multimedia Applications", Technical Report CSL-TR-97-721, Computer Systems Laboratory, Stanford University, Apr. 1997.
114. Jason Nieh and Monica S. Lam, "The SMART Scheduler", Project Technical Report SML-96-0213, Sun Microsystems Laboratories, July 1996.
115. Jason Nieh and Monica S. Lam, "The Design of SMART: A Scheduler for Multimedia Applications", Technical Report CSL-TR-96-697, Computer Systems Laboratory, Stanford University, June 1996.
116. Jason Nieh, Monica S. Lam, and J. Duane Northcutt, "A Practical Unified Approach to Processor Scheduling", Project Technical Report SML-94-0488, Sun Microsystems Laboratories, Dec. 1994.
117. Jason Nieh and Marc Levoy, "Volume Rendering on Scalable Shared-Memory MIMD Architectures", Technical Report CSL-TR-92-537, Computer Systems Laboratory, Stanford University, Aug. 1992.
118. Brian LaMacchia and Jason Nieh, "The Standard Map Machine", AI Memo 1165, AI Laboratory, Massachusetts Institute of Technology, Sept. 1989.
119. Jason Nieh, "Using Special-Purpose Computing to Examine Chaotic Behavior in Nonlinear Mappings", AI Technical Report 1139, AI Laboratory, Massachusetts Institute of Technology, Sept. 1989.
120. Jason Nieh, "DMI Mode 3 Throughput Analysis", Technical Memorandum, AT&T Information Systems, Dec. 1987.
121. Jason Nieh, "Delay and Throughput", Memorandum for File, AT&T Information Systems, Oct. 1986.

SELECTED INVITED TALKS

Distinguished Lecture, School of Computing and Information Sciences, Florida International University, Miami, FL, Feb. 2009.

Keynote Speaker, VMAP Summit, VMworld 2008, Las Vegas, NV, Sept. 2008.

Invited External Speaker, IBM System Software Day, IBM Watson Research Center, Yorktown Heights, NY, Sept. 2008.

Bell Laboratories, Alcatel-Lucent, Murray Hill, NJ, Nov. 2007.

Keynote Panel, VMworld 2006, Los Angeles, CA, Nov. 2006.

ITL Colloquium, National Institute of Standards and Technology (NIST), Washington, DC, June 2005.

DARPA ISAT Meeting, Washington, DC, June 2005.

CERCS Colloquium, Georgia Institute of Technology, Atlanta, GA, May 2005.

Invited Talk, 2005 USENIX Annual Technical Conference, Anaheim, CA, Apr. 2005.

DCS Colloquium, Rutgers University, Rutgers, NJ, Feb. 2005.

Young Investigator Lecture, 2004 Sigma Xi Annual Meeting, Montreal, Quebec Canada, Nov. 2004.

URCS Seminar, University of Rochester, Rochester, NY, Nov. 2004.

Systems Design and Implementation / Laboratory for Computer Systems (SDI/LCS) Seminar, Carnegie Mellon University, Pittsburgh, PA, Oct. 2004.

OS-PIC, IBM Watson Research Center, Yorktown Heights, NY, Oct. 2003.

MIT Workshop on Streaming Systems, Dedham, MA, Aug. 2003.

Hewlett-Packard Laboratories, Palo Alto, CA, June 2002.

Panasonic Information and Networking Technologies Laboratory, Princeton, NJ, May 2001.

OS-PIC, IBM Watson Research Center, Yorktown Heights, NY, April 2001.

Telcordia, Morristown, NJ, Nov. 2000.

OS-PIC, IBM Watson Research Center, Yorktown Heights, NY, May 2000.

Digital Equipment Systems Research Center, Palo Alto, CA, May 1998.

Division of Engineering and Applied Sciences, Harvard University, Cambridge, MA, May 1998.

Dept. of Computer Science, Yale University, New Haven, CT, Apr. 1998.

Dept. of Computer Science, Brown University, Providence, RI, Apr. 1998.

Dept. of Computer Science, University of Illinois at Urbana-Champaign, Urbana, IL, Apr. 1998.

Dept. of Computer and Information Science, University of Pennsylvania, Philadelphia, PA, Apr.1998.

Dept. of Computer Science, University of Toronto, Toronto, Ontario, Canada, Apr. 1998.

Dept. of Computer Science, New York University, New York, NY, Mar. 1998.

Dept. of Computer Science, Northwestern University, Evanston, IL, Mar. 1998.

Hewlett-Packard Laboratories, Palo Alto, CA, June 1997.

Computer Forum Annual Meeting, Stanford University, Stanford, CA, Mar. 1997.

Computer Science Colloquium, University of California at Santa Barbara, Santa Barbara, CA, Mar. 1997.

IEEE RTSS Workshop on Resource Allocation Problems in Multimedia Systems, Washington, DC, Dec. 1996.

Distributed Systems Seminar, Stanford University, Stanford, CA, Apr. 1994.

Sun Microsystems Laboratories, Mountain View, CA, Oct. 1993.

Hewlett-Packard Laboratories, Palo Alto, CA, Oct. 1992.

Scientific Visualization Seminar, NASA Ames Research Center, Mountain View, CA, Sept. 1992.

PROFESSIONAL ACTIVITIES

EDITORIAL BOARDS

Member, Editorial Board, *IEEE Internet Computing*, 2008 - present.

Guest Editor, Special Issue on Virtual Machines, *IEEE Pervasive Computing*, Oct.-Dec. 2009.

Member, Editorial Board, *Computer Networks Journal (COMNET)*, 2006 - 2008.

CONFERENCE PROGRAM COMMITTEES

Member, Program Committee, *30th Annual IEEE Conference on Computer Communications (Infocom 2011)*, Shanghai, China, Apr. 10-15, 2011.

Member, Program Committee, *16th International Conference on Mobile Computing and Networking (MobiCom 2010)*, Chicago, IL, Sept. 20-24, 2010.

Member, Program Committee, *International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2010)*, New York, NY, June 14-18, 2010.

Member, Program Committee, *3rd Annual Haifa Experimental Systems Conference (SYSTOR 2010)*, Haifa, Israel, May 24-26, 2010.

Member, Program Committee, *29th Annual IEEE Conference on Computer Communications (Infocom 2010)*, San Diego, CA, Mar. 15-19, 2010.

Member, Program Committee, *8th USENIX Conference on File and Storage Technologies (FAST 2010)*, San Jose, CA, Feb. 23-26, 2010.

Member, Program Committee, *2nd Workshop on Hot Topics in Software Upgrades (HotSWUp 2009)*, Orlando, FL, Oct. 2009.

Member, Program Committee, *1st Workshop on Networking, Systems, and Applications for Mobile Handhelds (MobiHeld 2009)*, Barcelona, Spain, Aug. 17, 2009.

Member, Program Committee, *2nd Workshop on Mobile Computing and Virtualization (MobiVirt 2009)*, Kraków, Poland, June 22, 2009.

Co-Chair, Program Committee, *Joint International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS / Performance 2009)*, Seattle, WA, June 15-19, 2009.

Member, Program Committee, *28th Annual IEEE Conference on Computer Communications (Infocom 2009)*, Rio de Janeiro, Brazil, Apr. 19-25, 2009.

Member, Program Committee, *2009 ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (VEE 2009)*, Washington, DC, Mar. 11-13, 2009.

Co-Chair, Program Committee, *1st ACM Workshop on Virtual Machine Security (VMSec 2008)*, Fairfax, VA, Oct. 31, 2008.

Member, Program Committee, *5th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous 2008)*, Dublin, Ireland, July 21-25, 2008.

Member, Program Committee, *1st Workshop on Mobile Computing and Virtualization (MobiVirt 2008)*, Breckenridge, CO, June 17, 2008.

Member, Program Committee, *International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2008)*, Annapolis, MD, June 2-6, 2008.

Member, Program Committee, *27th Annual IEEE Conference on Computer Communications (Infocom 2008)*, Phoenix, AZ, Apr. 13-18, 2008.

Member, Program Committee, *VMworld 2007*, San Francisco, Sept. 11-13, 2007.

Member, Program Committee, *13th International Conference on Mobile Computing and Networking (MobiCom 2007)*, Montreal, Quebec, Canada, Sept. 9-14, 2007.

Member, Program Committee, *2007 USENIX Annual Technical Conference (USENIX 2007)*, Santa Clara, CA, June 17-22, 2007.

Member, Program Committee, *International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2007)*, San Diego, CA, June 12-16, 2007.

Member, Program Committee, *2007 ACM/USENIX International Conference on Mobile Systems, Applications, and Services (MobiSys 2007)*, Puerto Rico, June 11-14, 2007.

Vice Chair, Program Committee, *16th International World Wide Web Conference (WWW2007)*, Banff, Alberta, Canada, May 8-12, 2007.

Member, Program Committee, *12th International Conference on Mobile Computing and Networking (MobiCom 2006)*, Los Angeles, CA, Sept. 24-29, 2006.

Member, Program Committee, *2006 IEEE International Conference on Cluster Computing (Cluster 2006)*, Barcelona, Spain, Sept. 25-27, 2006.

Member, Program Committee, *2006 USENIX Annual Technical Conference (USENIX 2006)*, Boston, MA, May 30-June 3, 2006.

Deputy Vice Chair, Program Committee, *15th International World Wide Web Conference (WWW2006)*, Edinburgh, UK, May 22-26, 2006.

Member, Program Committee, *International Conference on E-business and Telecommunication Networks (ICETE 2005)*, Reading, UK, Oct. 3-7, 2005.

Member, Program Committee, *International Work Conference on Next Generation Web Services Practices (NWeSP 2005)*, Seoul, Korea, Aug. 23-26, 2005.

Member, Program Committee, *IASTED International Conference on Web Technologies, Applications and Services (WTAS 2005)*, Calgary, Canada, July 4-6, 2005.

Member, Program Committee, *International Conference on Communications, Circuits and Systems (ICCCAS 2005)*, Hong Kong, China, May 27-30, 2005.

Member, Program Committee, *2005 USENIX Annual Technical Conference (USENIX 2005)*, Anaheim, CA, Apr. 10-15, 2005.

Member and WiPs Chair, Program Committee, *6th Symposium on Operating System Design and Implementation (OSDI 2004)*, San Francisco, CA, Dec. 6-8, 2004.

Member, Program Committee, *Multimedia Interactive Protocols and Systems (MIPS 2004)*, Grenoble, France, Nov. 16-19, 2004.

Member, Program Committee, *2nd International Conference on Service Oriented Computing (ICSOC 2004)*, New York, NY, Nov. 15-19, 2004.

Co-Chair, Program Committee, *1st ACM Workshop on Operating System and Architectural Support for the On Demand IT Infrastructure (OASIS 2004)*, Boston, MA, Oct. 9, 2004.

Member, Program Committee, *33rd International Conference on Parallel Processing (ICPP 2004)*, Montreal, Canada, Aug. 13-19, 2004.

Member, Program Committee, *International Conference on Communications, Circuits and Systems (ICCCAS 2004)*, Chengdu, China, June 27-29, 2004.

Member, Program Committee, *Joint International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS / PERFORMANCE 2004)*, New York, NY, June 12-16, 2004.

Deputy Vice Chair, Program Committee, *13th International World Wide Web Conference (WWW2004)*, New York, New York, May 17-22, 2004.

Member, Program Committee, *Multimedia Interactive Protocols and Systems (MIPS 2003)*, Napoli, Italy, Nov. 18-21, 2003.

Member, Program Committee, *13th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2003)*, Monterey, CA, June 1-3, 2003.

Member, Program Committee, *12th International World Wide Web Conference (WWW2003)*, Budapest, Hungary, May 20-24, 2003.

Member, Program Committee, *Joint International Workshop on Interactive Distributed Multimedia Systems / Protocols for Multimedia Systems (IDMS / PROMS 2002)*, Coimbra, Portugal, Nov. 26-29, 2002.

Member, Program Committee, *16th International Conference on Supercomputing (ICS 2002)*, New York, NY, June 22-26, 2002.

Member, Program Committee, *1st Workshop on Self-Healing, Adaptive and Self-MANaged Systems (SHAMAN 2002)*, New York, NY, June 23, 2002.

Member, Program Committee, *2002 USENIX Annual Technical Conference (USENIX 2002)*, Monterey, CA, June 9-14, 2002.

Member, Program Committee, *12th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2002)*, Miami Beach, FL, May 12-14, 2002.

Member, Program Committee, *8th International Workshop on Interactive Distributed Multimedia Systems (IDMS 2001)*, Lancaster, UK, Sept. 4-7, 2001.

Co-Chair, Program Committee, *11th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2001)*, New York, NY, June 25-26, 2001.

Member, Program Committee, *1st New York Metro Area Networking Workshop (NYMAN 2001)*, Hawthorne, NY, Mar. 12, 2001.

Member, Program Committee, *10th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2000)*, Chapel Hill, NC, June 26-28, 2000.

Member, Program Committee, *9th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 1999)*, Basking Ridge, NJ, June 23-25, 1999.

CONFERENCE STEERING AND ORGANIZING COMMITTEES

Member, Steering Committee, *15th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2005)*, Skamania, WA, June 12-14, 2005.

Local Organization Co-Chair, Organizing Committee, *2nd International Conference on Service Oriented Computing (ICSOC 2004)*, New York, NY, Nov. 15-19, 2004.

Co-Chair, Organizing Committee, *1st ACM Workshop on Operating System and Architectural Support for the On Demand IT Infrastructure (OASIS 2004)*, Boston, MA, Oct. 9, 2004.

Member, Steering Committee, *14th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2004)*, Cork, Ireland, June 16-18, 2004.

Publicity Chair, Organizing Committee, *Joint International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS / PERFORMANCE 2004)*, New York, NY, June 12-16, 2004.

Member, Steering Committee, *13th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2003)*, Monterey, CA, June 1-3, 2003.

University Liaison, Organizing Committee, *16th International Conference on Supercomputing (ICS 2002)*, New York, NY, June 22-26, 2002.

Member, Steering Committee, *12th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2002)*, Miami Beach, FL, May 12-14, 2002.

Co-Chair, Organizing Committee, *11th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2001)*, New York, NY, June 25-26, 2001.

JOURNAL AND CONFERENCE REFEREEING (in addition to conference program committees)

ACM Computing Surveys.

ACM Computer Communication Journal.

ACM Multimedia Conference.

ACM Multimedia Systems Journal.

ACM SIGGRAPH.

ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI).

ACM Symposium on Operating Systems Principles (SOSP).

ACM Symposium on Parallelism in Algorithms and Architectures (SPAA).

ACM Transactions on Computer Systems (TOCS).

ACM Transactions on Multimedia Computing, Communication, and Applications (TOMCCAP).

ACM Transactions on Internet Technology (TOIT).

The Computer Journal.

International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS).

IEEE GLOBECOM Technical Conference.

IEEE International Parallel and Distributed Processing Symposium (IPDPS).

IEEE Internet Computing.

IEEE Journal of Selected Areas in Communications.

IEEE Multimedia.

IEEE Transactions on Computers.

IEEE Transactions on Circuits and Systems for Video Technology.

IEEE Transactions on Mobile Computing.

IEEE Transactions on Multimedia.

IEEE Transactions on Parallel and Distributed Systems.

IEEE/ACM Transactions on Networking.

IEEE Transactions on Knowledge and Data Engineering.

IEEE Transactions on Software Engineering.

IEEE Wireless Communications and Networking Conference (WCNC).

International Conference on Dependable Systems and Networks (DSN).

International Workshop on Volume Visualization.

Journal of Parallel and Distributed Computing.

The Journal of Systems and Software.

Software Practice and Experience.

USENIX Annual Technical Conference.

USENIX Annual Technical Conference, FREENIX Track.

USENIX Conference on File and Storage Technologies (FAST).

USENIX Symposium on Networked Systems Design and Implementation (NSDI).

USENIX Security Symposium.

FUNDING AGENCIES

Participant, *NSF Cyber Trust PI Workshop*, New Haven, CT, 2008.

Participant, *NSF CISE PI Workshop*, Urbana, IL, 2005.

Participant, *NSF Cyber Trust PI Workshop*, Newport Beach, CA, 2005.

Participant, *DARPA ISAT "Law of Large Numbers System Design" Study Group*, 2005.

Grant Review Panelist, *National Science Foundation*, Arlington, VA, 2000 - 2005, 2009.

Participant, *NSF CISE PI Workshop*, Las Cruces, NM, 1999.

STANDARDIZATION COMMITTEES

Member, Net2Display Task Group, *Video Electronics Standards Association (VESA)*, 2005 - 2009.

Member, DPVL Task Group, *Video Electronics Standards Association (VESA)*, 2005 - 2006.

OUTREACH ACTIVITIES

Member, *VMAP Advisory Board*, VMware, 2009 - present.

Member, Executive Advisory Committee, *Harlem Children Society*, 2007 - present.

Mentor, Computing Innovation Fellows Project, 2009 - 2010.

Advisor, Online Membership Services Strategy, *Association for Computing Machinery*, 2007 - 2008.

Invitee, Infoscape Charrette, *Lincoln Center for the Performing Arts*, 2007.

Board Member, Membership Services Board, *Association for Computing Machinery*, 2004 - 2007.

Managing Group Member, Security and Infrastructure Standing Committee, *Financial Services Technology Consortium (FSTC)*, 2006 - 2007.

Examiner, Graduate Record Examinations (GRE) Computer Science Test, *Educational Testing Service*, 2004 - 2005.

Judge, New York City Science and Engineering Fair (NYCSEF), *New York Academy of Sciences*, 2004.

Mentor, Harlem Children Society Internship Program, *Harlem Children Society*, 2006.

Mentor, Science Research Training Program, *New York Academy of Sciences*, 2001 - 2003, 2006.

Faculty Mentor, Summer Research Program for Historically Underrepresented Groups, *Leadership Alliance,* 2000.

PROFESSIONAL SOCIETIES

Member, Association for Computing Machinery (ACM).

Senior Member, Institute of Electrical and Electronic Engineers (IEEE).

Member, New York Academy of Sciences.

Member, USENIX Association.

UNIVERSITY ACTIVITIES

(all activities at Columbia University unless otherwise noted)

DOCTORAL DISSERTATIONS SUPERVISED

1. Nicolas Viennot, Sept. 2010 - present.
2. Jeremy Andrus, Sept. 2010 - present.
3. Dan Phung, June 2004 - present.
4. Oren Laadan, Sept. 2003 - present (SEAS Presidential Fellow 2003-2007).
5. Dinesh Subhraveti, Sept. 2001 - present.
6. Alexander Sherman, "Guaranteeing Performance through Fairness in Peer-to-Peer File Sharing and Streaming Systems", Ph.D. Computer Science, defended Oct. 2009.
7. Shaya Potter, "Virtualization Mechanisms for Mobility, Security, and System Administration", Ph.D. Computer Science, May 2010, currently Postdoctoral Scholar, IBM T.J. Watson Research Center.
8. Haoqiang Zheng, "CPU Scheduling with Automatic Interactivity and Dependency Detection", Ph.D. Computer Science, defended July 2009, currently Senior Staff Engineer, VMware.
9. Ricardo Baratto, "THINC: A Virtual and Remote Display Architecture for Desktop Computing", Ph.D. Computer Science, defended Oct. 2007 (with distinction), currently Senior Software Engineer, Calista Technologies.
10. Albert M. Lai, "A Remote Training Approach for Teaching Seniors to Use a Telehealth System", Ph.D. Biomedical Informatics, Feb. 2007 (with distinction, co-advised with Justin Starren), currently Assistant Professor, Department of Biomedical Informatics, Ohio State University.
11. David P. Olshefski, "Measuring and Managing the Remote Client Perceived Response Time for Web Transactions using Server-side Techniques", Ph.D. Computer Science, Oct. 2006 (with distinction), currently Research Staff Member, IBM T.J. Watson Research Center.
12. Gong Su, "MOVE: Mobility with Persistent Network Connections", Ph.D. Computer Science, Oct. 2004, currently Research Staff Member, IBM T.J. Watson Research Center.
13. Erez Zadok, "FiST: A System for File System Code Generation", Ph.D. Computer Science, May 2001, currently Associate Professor, Department of Computer Science, Stony Brook University.

OTHER DOCTORAL DISSERTATION COMMITTEES

1. Rean Griffith, "Evaluating Software Systems via Runtime Fault-Injection and Reliability, Availability and Serviceability (RAS) Metrics and Models", Ph.D. Computer Science, Oct. 2008.
2. Stelios Sidiroglou, "Software Self-Healing Using Error Virtualization", Ph.D. Computer Science, May 2008.
3. Jacob Gorm Hansen, "Virtual Machine Mobility with Self-Migration", Ph.D. Computer Science, University of Copenhagen, Feb. 2008.
4. Hanhua Feng, "Scheduling: From Optimality to Configurability", Ph.D. Computer Science, Feb. 2008.
5. Sangho Shin, "Towards the Quality of Service for VoIP traffic in IEEE 802.11 Wireless Networks", Ph.D. Computer Science, Feb. 2008.
6. Aniruddha Bohra, "System Architectures Based on Functionality Offloading", Ph.D. Computer Science, Rutgers University, Jan. 2008.
7. Hoon Chang, "Incorporating Physical Layer Capture in the Modeling, Analysis and Design of Wireless Access Mechanisms", Ph.D. Computer Science, May 2007.
8. Xiaotao Wu, "Ubiquitous Programmable Internet Telephony End System Services", Ph.D. Computer Science, May 2007.
9. Weibin Zhao, "Towards Autonomic Computing: Service Discovery and Web Hotspot Service", Ph.D. Computer Science, May 2006.
10. Daniel Villela, "Resource Management in Large-Scale Services: Models and Algorithms", Ph.D. Electrical Engineering, Feb. 2006.

11. Yong Wang, “Resource Constrained Video Coding/Adaptation”, Ph.D. Electrical Engineering, Feb. 2006.
12. Giuseppe Valetto, “Orchestrating the Dynamic Adaptation of Distributed Software with Workflow Technology”, Ph.D. Computer Science, May 2004.
13. Lisa Amini, “Models and Algorithms for Resource Management in Distributed Computing Cooperatives”, Ph.D. Computer Science, Feb. 2004.
14. Jonathan Lennox, “Services for Internet Telephony”, Ph.D. Computer Science, Feb. 2004.
15. Raymond Liao, “Utility-Based Adaptation, Dynamic Provisioning and Incentive Engineering Techniques for Internet and its Wireless Extensions”, Ph.D. Electrical Engineering, May 2003.
16. Sushil da Silva, “Netscript: A Language System for Active Networks”, Ph.D. Computer Science, May 2003.
17. Maria Papadopouli, “Resource Sharing in Mobile Wireless Networks”, Ph.D. Computer Science, Oct. 2002.
18. Denes Molnar, “Classical Transport Theory and Its Applications in Heavy-ion Physics”, Ph.D. Physics, July 2002.
19. Apostolos Dailianas, “MarketNet: A Survivable, Market-Based Architecture for Large-Scale Information Systems”, Ph.D. Computer Science, Jan. 2001.
20. Steve Dossick, “A Virtual Environment Framework for Software Engineering”, Ph.D. Computer Science, Nov. 2000.

OTHER DOCTORAL EXAM COMMITTEES

1. Omer Boyaci, “Multimedia Tools for Application Sharing, Measuring Capture-to-display Latency, and User Created Services”, Mar. 2010 (Thesis Proposal Committee).
2. Omer Boyaci, “Multimedia Collaboration and Application Sharing”, June 2008 (Candidacy Exam Committee).
3. Stelios Sidiroglou, “Error Virtualization: A Technique for Autonomic Software Self-Healing”, Dec. 2006 (Thesis Proposal Committee).
4. Hanhua Feng, “Optimal Stochastic Scheduling”, Dec. 2006 (Thesis Proposal Committee).
5. Hoon Chang, “Analytical Model and Fairness Scheduling of CSMA/CA in Physical Layer Capturing”, May 2006 (Thesis Proposal Committee).
6. Michael Locasto, “A Virtual CPU Framework for Self-Healing Software”, Dec. 2005 (Thesis Proposal Committee).
7. Stelios Sidiroglou, “Common Mode Attacks”, Nov. 2005 (Candidacy Exam Committee).
8. Rean Griffith, “Design and Implementation of Self-healing Systems”, Nov. 2004 (Candidacy Exam Committee).
9. Daniel Villela, “Resource Management for Services in Federated Systems”, Apr. 2004 (Thesis Proposal Committee).
10. Weibin Zhao, “Advanced Service Discovery and Web Hotspot Rescue”, May 2003 (Thesis Proposal Committee).
11. Lisa Amini, “Algorithms and Protocols for Content Internetworking”, Jan. 2002 (Thesis Proposal Committee).
12. Xiaotao Wu, “Telecommunication Services”, Nov. 2001 (Candidacy Exam Committee).
13. Lisa Amini, “Distributed Content Services Framework”, Dec. 2000 (Candidacy Exam Committee).
14. Eleazar Eskin, “Probabilistic Approaches of Anomaly Detection Applied to Intrusion Detection”, May 2000 (Candidacy Exam Committee).
15. Giuseppe Valetto, “Formalisms and Mechanisms for Specifying and Supporting Coordination in Distributed Systems”, Apr. 2000 (Candidacy Exam Committee).
16. Jonathan Lennox, “Advanced Services for Internet Telephony” Feb. 2000 (Thesis Proposal Committee).
17. Weibin Zhao, “Internet Quality of Service”, Dec. 1999 (Candidacy Exam Committee).
18. Alexander Konstantinou, “Computational Models of Change Propagation”, Dec. 1999 (Candidacy Exam Committee).
19. Ping Pan, “On Scalable Internet Resource Reservation”, Apr. 1999 (Candidacy Exam Committee).

MASTERS DISSERTATIONS SUPERVISED

1. Lei Zhang, “Implementing A Windows Remote Display Architecture”, M.S. Computer Science, Feb. 2006.

2. Bogdan Caprita, “Grouped Distributed Queues: Distributed Queue, Proportional Share Multiprocessor Scheduling”, M.S. Computer Science, May 2005.
3. V. Guruprasad, “Canonical Simplification and Automation of the Internet”, M.S Computer Science, May 2005.
4. Wong Chun Chan, “Group Ratio Round-Robin: An O(1) Proportional Share Scheduler”, M.S. Computer Science, June 2004.
5. Erik Hogstedt, “Implementing ALM: an Application-level Multicast Protocol for Group Work and Group Study”, M.S. Media Technology, Royal Institute of Technology, Stockholm, Sweden, June 2002.

OTHER MASTERS DISSERTATION COMMITTEES

1. Stephen Boyd, “Practical Randomization Techniques For Combatting Code-Injection Attacks”, M.S. Computer Science, May 2004.

MASTERS PROJECT STUDENTS SUPERVISED

1. Carlos Perez, M.S. Computer Science, expected May 2010 (published in *ASPLOS 2009*).
2. Jau-Yuan Chen, M.S. Computer Science, Feb. 2010.
3. Christoffer Dall, M.S. Computer Science, Feb. 2010.
4. Sinan Xiao, M.S. Computer Science, Feb. 2010.
5. Xintong Zhou, M.S. Computer Science, Feb. 2010.
6. Daniel Benamy, M.S. Computer Science, May 2009.
7. Andreas Nilsson, M.S. Computer Science, May 2009.
8. Adrian Frei, M.S. Computer Science, Feb. 2009.
9. Ke Jin, M.S. Computer Science, Feb. 2009.
10. Shariar Kazi, M.S. Computer Science, Feb. 2009.
11. Taek Joo Kim, M.S. Computer Science, Feb. 2009.
12. John Morales, M.S. Computer Science, Feb. 2009.
13. Shrinivas Nidadavolu, M.S. Computer Science, Feb. 2009.
14. Nicolas Viennot, M.S. Computer Science, Feb. 2009 (published in *ASPLOS 2009*).
15. Ken Lee, M.S. Computer Science, May 2008.
16. Divya Arora, M.S. Computer Science, Feb. 2008.
17. Jayesh Kataria, M.S. Computer Science, Feb. 2008.
18. Amortya Ray, M.S. Computer Science, Feb. 2008.
19. Dhruva Shetty, M.S. Computer Science, Feb. 2008.
20. Tarandeep Singh, M.S. Computer Science, Feb. 2008.
21. Young Jin Yoon, M.S. Computer Science, Feb. 2008.
22. Joon Seong Ahn, M.S. Computer Science, Oct. 2007.
23. Ilho Ye, M.S. Computer Science, Feb. 2007.
24. Nabahwaya Bashir-Bello, M.S. Computer Science, Feb. 2006.
25. Joeng Kim, M.S. Computer Science, Feb. 2006 (published in *WWW2006, SCC 2006*).
26. Pinxing Ye, M.S. Computer Science, Feb. 2006.
27. Sarita Bafna, M.S. Computer Science, May 2005.
28. Jonah Benton, M.S. Computer Science, May 2005.
29. Bhaygyashree Bohra, M.S. Computer Science, May 2005 (published in *WWW2004*).
30. Pavan-Kumar Josyula-Venkata, M.S. Computer Science, May 2005.

31. Leonard Kim, M.S. Computer Science, May 2005 (published in *SOSP 2005*).
32. Vijayarka Nandikonda, M.S. Computer Science, May 2005 (published in *WWW2004*).
33. Madhuri Shinde, M.S. Computer Science, May 2005.
34. Abhishek Surana, M.S. Computer Science, May 2005 (published in *WWW2004*).
35. Suchita Varshneya, M.S. Computer Science, May 2005 (published in *WWW2004*).
36. Raghu Arur, M.S. Computer Science, May 2004.
37. Paul Henley, M.S. Computer Science, May 2004.
38. Yong Gao, M.S. Computer Science, May 2003.
39. Shilpa Krishnappa, M.S. Computer Science, May 2003 (published in *WWW2003*).
40. Aparna Mohla, M.S. Computer Science, May 2003 (published in *WWW2003*).
41. Mahdi Sajjadpour, M.S. Electrical Engineering, May 2003 (published in *WWW2003*).
42. Nikhil Tiwari, M.S. Computer Science, May 2003 (published in *USENIX 2002*).
43. S. Jae Yang, M.S. Computer Science, in progress (published in *NOSSDAV 2000*, *PC Magazine 2001*, *USENIX 2001*, *PC Magazine 2002*, *USENIX 2002*, *TOCS 2003*, *WWW2003*).
44. Ravi Gadhia, M.S. Computer Science, Feb. 2003.
45. Jianqin Qu, M.S. Computer Science, May 2002.
46. Fei Li, M.S. Computer Science, Jan. 2002 (published in *DCC 2002*, *ICC 2002*).
47. Albert Lai, M.S. Computer Science, May 2001 (published in *SIGMETRICS 2002, TOCS 2006*).
48. Chris Vaill, M.S. Computer Science, May 2001 (published in *USENIX 2001*, *SIGCSE 2005, OSR 2006*).
49. Hua Zhong, M.S. Computer Science, May 2001 (published in *USENIX 2001*).
50. Rahul Joshi, M.S. Computer Science, Feb. 2001.
51. Yuan Liu, M.S. Computer Science, Oct. 2000.
52. Johan M. Andersen, M.S. Computer Science, May 2000 (published in *USENIX 2001*).
53. Sung Hyun Cho, M.S. Computer Science, May 2000.
54. Du Hee Lee, M.S. Computer Science, May 2000.
55. Naomi Novik, M.S. Computer Science, May 2000 (published in *USENIX 2001*, *TOCS 2003*).
56. Ari Steinfeld, M.S. Computer Science, May 2000.
57. Yue Hai Tan, M.S. Computer Science, Feb. 2000.

UNDERGRADUATE DISSERTATIONS SUPERVISED

1. Matthew Selsky, "Creating Secure Partitions for Virtualized Migration Environments", B.S. Computer Science, May 2005.

UNDERGRADUATE PROJECT STUDENTS SUPERVISED

1. David Alpert, B.S. Computer Science, May 2009.
2. Jordan Rupprecht, B.S. Computer Science, May 2009.
3. Arjun Roy, B.S. Computer Science, May 2009.
4. Andrew Shu, B.S. Computer Science, May 2009.
5. Matt Schulkind, B.S. Computer Science, May 2006.
6. Bok-Lyn Wong, B.S. Computer Science, Feb. 2006.
7. Bogdan Caprita, B.S. Computer Engineering and B.S. Applied Mathematics, Feb. 2005 (Computing Research Association's Outstanding Undergraduate Award 2004/2005 Finalist, 2005 Theodore R. Bashkow Award, published in *ANCS 2005*, *USENIX 2005*).

8. Yuly Finkelberg, B.S. Computer Science, May 2005.
9. Irina Likhtina, B.S. Computer Science, May 2005.
10. Robert Tobkes, B.S. Computer Science, May 2005.
11. Tony Capra, B.A. Computer Science, May 2004.
12. Dave Coulthart, B.S. Computer Science, May 2004.
13. Hubert Lin, B.S. Computer Science, May 2004.
14. Dong Lou, B.S. Computer Science, May 2004.
15. Jen Wang, B.S. Computer Science, May 2004.
16. Gerardo Flores, B.S. Computer Science, May 2003.
17. Leonard Kim, B.S. Computer Science, May 2003.
18. Sung Y. Cho, B.S. Computer Science, May 2002.
19. Erik Czernikowski, B.S. Computer Science, May 2002.
20. Aner Fust, B.S. Computer Science, May 2002.
21. Michael Kalnicki, B.S. Computer Science, May 2002.
22. Eugene Kim, B.S. Computer Science, May 2002.
23. Ilia Malkovitch, B.S. Computer Science, May 2002.
24. Steven Osman, B.S. Computer Science, May 2002 (published in *OSDI 2002*).
25. Francesco Tamburrino, B.S. Electrical Engineering, Feb. 2002.
26. Paolo de Dios, B.S. Computer Science, May 2001.
27. Carla Goldburg, B.A. Computer Science, May 2001.
28. Sara Schumacher, B.A. Computer Science, Feb. 2001.
29. Ozgur Can Leonard, B.S. Computer Science, May 2000 (published in *Dr. Dobb's Journal 2000*).

UNIVERSITY SERVICE

Member, SEAS Faculty Advisory Committee for Entrepreneurship, 2007 - present.

Faculty Advisor, Society for Entrepreneurship and Technological Innovation at Columbia University (SETI), 2008 - 2009.

Member, SEAS Nominating Committee, 2005 - 2007.

Member, Senate Committee on Athletic Eligibility, 2001 - 2008. Served on provost-appointed committee responsible for general policy on athletic eligibility and ruling on student appeals to be able to participate despite falling short of the Columbia standard for degree progress.

Member, Faculty Focus Group on Child Care, Office of Planning and Institutional Research, 2005.

Faculty Volunteer, Urban New York, Office of Student Activities, 2003 - 2007, 2010.

Member, RASCAL Project Advisory Committee, 1999 - 2001. Served on advisory committee responsible for providing guidance and feedback on the design of the electronic research administration system (RASCAL), now in use by the Office of Projects and Grants, https://www.rascal.columbia.edu.

Undergraduate Associate Advisor, Massachusetts Institute of Technology, 1987 - 1988.

DEPARTMENTAL SERVICE (Dept. of Computer Science unless otherwise noted)

Member and Chair, Visibility Committee, 2009 - present (Chair, 2009).

Member, Academic Committee, 2003 - 2006, 2008 - present.

USENIX Campus Liaison, USENIX Association, 2004 - present.

Faculty Organizer and Speaker, Professional Preparation Seminar Series, 2008 - 2009.

Co-Chair, Faculty Retreat, 2008.

Lab Demonstrations, Undergraduate and MS Research Project Fair, 2008.

Member and Chair, Strategic Planning Committee, 2005 - 2008 (Chair, 2007 - 2008).

Speaker, ACM Luncheon and Research Series, 2008.

Member, Faculty Recruiting Committee, 2003 - 2008.

Member and Chair, Facilities Committee, 1999 - 2006 (Chair, 2002 - 2003).

Faculty Advisor, Columbia Mainframe Computing Group, 2005 - 2006.

Member, Bill Campbell Visit Organizing Committee, 2005.

Member, Faculty Retreat Organizing Committee, 2005.

Department Representative, NSF CISE Workshop, 1999, 2005.

Member, Academic Honesty Task Force, 2004 - 2005.

Editor-in-Chief, 25th Anniversary of the Department of Computer Science Newsletter, 2004 - 2005.

Operating Systems Comprehensive Examiner, 1999 - 2004.

Speaker Host, 25th Anniversary Distinguished Lecture Series, 2004.

Lab Demonstrations, 25th Anniversary of the Department of Computer Science, 2004.

Speaker, 25th Anniversary of the Department of Computer Science, 2004.

Columbia College Academic Advisor (Seniors), 2003 - 2004.

Lab Demonstrations, ACM Computer Science Research Fair, 2003.

Ph.D. Funding Survey, Ph.D. Committee, 2003.

Chair, CRF Director Search Committee, 2003.

Columbia College Academic Advisor (Juniors), 2002 - 2003.

Departmental Infrastructure and Systems Area Speaker, External Review, 2003.

Research Demonstration, CAP Computer Science Research Fair, 2002.

Speaker, ACM Computer Science Research Fair, 2002.

Speaker, Faculty Research Colloquia, 2002.

Faculty Assistant Manager, 2000 - 2002.

Columbia College Academic Advisor (Freshman and Sophomores), 2001 - 2002.

Member, Ph.D. Admissions Committee, 1999 - 2002.

Speaker, ACM Computer Science Research Fair, 2001.

Speaker, Faculty Research Colloquia, 2001.

M.S. Academic Advisor, 1999 - 2001.

Department Faculty Representative, SEAS Engineering Council, 2001.

Speaker, ACM Computer Science Research Fair, 2000.

SEAS New Graduate Student Orientation, 2000.

Computer Science Colloquium Chair, 1999 - 2000. Faculty comments: "This seems to have been the most interesting set of colloquia since I've been at Columbia." (Feb. 2000). "I keep having to change plans because you've organized such a terrific colloquium series." (Feb. 2000). "Just fyi, that was one of the best colloquia I've ever been to in my life!" (Dec. 1999).

SEAS Alumni Faculty-Student Dinners, 1999.

Graduate Admissions Committee, Dept. of Electrical Engineering, Stanford University, 1996.

Graduate Mentor, Dept. of Electrical Engineering, Stanford University, 1993 - 1995.

CURRICULUM AND TEACHING

(all activities at Columbia University unless otherwise noted)

NEW CURRICULUM DEVELOPMENT

COMS E6998 Mobile Computing with iPhone and Android, 2008 - present. Developed and taught a new course on smartphone mobile computing that explores the technologies and convergence of computing, telephony, and sensors in the physical world. Course has also been profiled in:

Elizabeth Woyke, "iPhone and Android Apps 101", *Forbes.com*, New York, NY, Nov. 2008.

COMS E6998 Virtual Machines, 2007 - 2008. Co-developed and taught a new advanced graduate course on virtual machines.

COMS E6998 Topics in Computer Systems, 2005 - 2006. Developed and taught a new advanced graduate course on topics in computer systems which focuses on a different technical area of interest each semester.

COMS W4118 Operating Systems, 1999 - 2004. Developed and taught a new advanced undergraduate / graduate course in operating systems, which integrates operating system concepts with real-world operating system design and implementation. First course in the world to employ novel virtual machine technology to provide hands-on operating system design and implementation instruction in a real commercial operating system for both on-campus and distance learning students. Approach has been emulated at several other universities, including Calvin College, Clarkson University, John Hopkins University, SUNY Stony Brook, Swarthmore College, University of Illinois, University of Rochester, University of Virginia, University of Washington, Worcester Polytechnic Institute, etc. "The best CS class of my college career, both in terms of how much I learned and how valuable the information turned out to be in the real world. Writing new system calls, device drivers, schedulers... Mention to an interviewer that you know how to do this and they drool...", *Slashdot*, Dec. 2000. Course has also been profiled in:

"Software Doubles as Insurance Policy for Columbia University", *College Planning and Management*, Apr. 2001.

Charles Babcock, "VMware Welcomes Guest OSes", *Inter@ctive Week*, 7(17), Ziff-Davis Media, New York, NY, May 1, 2000, p. 86.

Mara Velasco Sweet, "Columbia Students Gain Valuable Experience in Operating System Design Using VMware", *VMware Customer Success Stories*, VMware, Palo Alto, CA, Oct. 1999.

COMS E6118 Advanced Operating Systems, 2000 - 2004. Developed and taught a new advanced graduate course in operating systems. New classroom and lab course materials were developed on recent research developments in operating systems. Course also develops research skills by emphasizing classroom discussion, student presentation skills, and in-depth programming projects.

COMS W3157 Advanced Programming, 2001. Helped formulate and develop an undergraduate advanced programming course with an emphasis on systems programming principles and tools.

COMS W3139 Data Structures and Algorithms in Java, 1999. Developed and taught a new undergraduate course in data structures and algorithms using Java. Previous versions of the course were taught in C, but a department decision to move the core undergraduate computer science curriculum to Java created a critical need for this course. New Java-based course materials were developed and have been subsequently been used by other faculty for this course.

TEACHING EXPERIENCE

COMS W3998 Projects in Computer Science, Fall 2000 - present. Enrollment 2 (Fall 2000), 1 (Spring 2001), 1 (Fall 2001), 2 (Spring 2002), 1 (Fall 2002), 2 (Spring 2003), 2 (Fall 2003), 3 (Spring 2004), 2 (Fall 2004), 1 (Fall 2005).

COMS W4901 Projects in Computer Science, Summer 1999 - present. Enrollment 1 (Summer 1999), 3 (Spring 2000), 2 (Summer 2000), 3 (Spring 2001), 1 (Fall 2001), 2 (Spring 2002), 3 (Spring 2003), 2 (Fall 2003), 2 (Fall 2005), 1 (Fall 2006), 4 (Fall 2008), 3 (Spring 2009).

COMS E6901 Projects in Computer Science, Spring 1999 - present. Enrollment 1 (Spring 1999), 8 (Fall 1999), 7 (Spring 2000), 2 (Summer 2000), 4 (Fall 2000), 4 (Spring 2001), 6 (Fall 2001), 6 (Spring 2002), 10 (Fall 2002), 5 (Spring 2003), 11 (Fall 2003), 2 (Spring 2004), 6 (Fall 2004), 6 (Spring 2005), 1 (Fall 2005), 3 (Spring 2006), 7 (Fall 2006), 2 (Spring 2007), 2 (Fall 2007), 6 (Spring 2008), 5 (Fall 2008) 4 (Spring 2009), 1 (Summer 2009), 1 (Fall 2009), 2 (Spring 2010).

COMS E6118 Advanced Operating Systems, Spring 2010. Enrollment 5 (2 CVN).

COMS W4118 Operating Systems, Fall 2009. Enrollment 65 (7 CVN), instructor rating 4.1/5.0.

COMS E6998 Mobile Computing with iPhone and Android, Summer 2009. Enrollment 4 (CVN pre-taped).

COMS W4118 Operating Systems, Summer 2009. Enrollment 8 (CVN pre-taped).

COMS E6998 Mobile Computing with iPhone and Android, Spring 2009. Enrollment 70 (14 CVN), instructor rating 3.9/5.0.

COMS W4118 Operating Systems, Fall 2008. Enrollment 74 (13 CVN), instructor rating 4.5/5.0.

COMS E6998 Virtual Machines, Spring 2008. Enrollment 24 (6 CVN), instructor rating 4.8/5.0.

COMS W4118 Operating Systems, Fall 2007. Enrollment 42, instructor rating 4.1/5.0.

COMS E6998 Topics in Computer Systems, Spring 2006. Enrollment 7, instructor rating 5.0/5.0.

COMS E6118 Advanced Operating Systems, Fall 2005. Enrollment 13, instructor rating 4.4/5.0.

COMS W4118 Operating Systems, Fall 2004. Enrollment 100 (16 CVN), instructor rating 4.3/5.0.

COMS W4118 Operating Systems, Summer 2004. Enrollment 4 (CVN pre-taped).

COMS E6118 Advanced Operating Systems, Spring 2004. Enrollment 22, instructor rating 4.3/5.0.

COMS W4118 Operating Systems, Fall 2003. Enrollment 83 (10 CVN), instructor rating 4.2/5.0.

COMS W4118 Operating Systems, Summer 2003. Enrollment 2 (CVN pre-taped).

COMS W4118 Operating Systems, Spring 2003. Enrollment 75 (5 CVN), instructor rating 4.2/5.0.

G22.3813 Advanced Laboratory in Computer Science, New York University, Spring 2003. Enrollment 1.

COMS W4118 Operating Systems, Fall 2002. Enrollment 84 (14 CVN), instructor rating 4.2/5.0.

COMS W4118 Operating Systems, Summer 2002. Enrollment 7 (CVN pre-taped).

COMS E6118 Advanced Operating Systems, Spring 2002. Enrollment 17, instructor rating 4.4/5.0.

COMS W4118 Operating Systems, Spring 2002. Enrollment 6 (CVN pre-taped).

COMS W4118 Operating Systems, Fall 2001. Enrollment 102 (16 CVN), instructor rating 4.1/5.0.

COMS W4118 Operating Systems, Summer 2001. Enrollment 8 (CVN pre-taped).

COMS E6118 Advanced Operating Systems, Spring 2001. Enrollment 5, instructor rating 4.4/5.0.

COMS W4118 Operating Systems, Fall 2000. Enrollment 127 (19 CVN), instructor rating 3.8/5.0.

COMS E6118 Advanced Operating Systems, Spring 2000. Enrollment 23, instructor rating 3.9/5.0.

COMS W4118 Operating Systems, Fall 1999. Enrollment 119 (11 CVN), instructor rating 3.8/5.0.

COMS E6901 Operating Systems and Networking Reading Seminar, Fall 1999.

COMS W3139 Data Structures and Algorithms in Java, Spring 1999. Enrollment 52, instructor rating 4.2/5.0. (nominated for Columbia Great Teacher Award)

Intermediate Guitar, Christian Guitarist Conference, Apr. 1996, 1997, 1998.

SELECTED STUDENT COURSE EVALUATION COMMENTS

"Great teaching and organization, the best CS course." (Fall 2009)

"I got to learn the most out of any course in my 2 years at Columbia." (Fall 2009)

"A true master of the subject matter; excellent classroom delivery; and unafraid to innovate around the homework assignments (Android, Git, VMs, etc)." (Fall 2009)

"I had Jason Nieh for both Operating Systems and this course. He is a great lecturer that really knows how to motivate students to learn." (Spring 2009)

"I love the concept of the class and I believe it's vital for students to continue broadening their skill sets to encompass more than just your usual CS topics. There was a lot of self-exploration but I felt that Professor Nieh did an excellent job keeping everyone engaged for the entire semester. That surely isn't easy." (Spring 2009)

"I'm so glad I took this course. It was so much fun...amazing course." (Spring 2009)

"Professor Nieh is the best professor I've studied under at Columbia University. His high standards boundless energy and ability to draw students into the lecture are amazing. His class is known for being the toughest and most demanding in our program. Yet I looked forward each day to attending his lectures and attacked the difficult problem sets with motivation and vigor unlike any other class. He inspires students to do the tough work not unlike the manner in which an athletic coach pushes and motivates his or her players. I wanted to do well in this class wanted to pull the countless all nighters if for no other reason then having the pride and incredible sense of accomplishment that comes with being able to hang with Jason Nieh. We need more professors like this who are able to set incredibly high standards while also inspiring students to achieve them while at the same time leaving the student with a very solid understanding of theory and very marketable skills." (Fall 2008)

"This course is the best CS course I have ever taken...Jason is an excellent teacher, who is very approachable and answers any question with insight and dedication, so take this course with him if you have the chance." (Fall 2008)

"This is by far the most demanding and rewarding class I have taken as a CS grad student at Columbia." (Fall 2008)

"Prof. Nieh is amazingly knowledgeable in this area and is able to communicate the material in an effective interesting manner that truly captivates students attention. Undoubtedly the best CS lecturer I have come across at Columbia." (Fall 2008)

"The best instructor I've encountered at CU." (Fall 2008)

"OS is the most thorough classes I've taken and has taught me the most." (Fall 2008)

"Prof. Nieh really knows his stuff and has some pretty amazing homework lined up. You can tell he put a lot of work into designing problems that seem plausible and teach you a lot. Much to my classmates chagrin I d say the homework is the best part of the class." (Fall 2008)

"...the best course I have taken. So much to learn and the hands-on Linux kernel development is fantastic." (Fall 2008)

"Professor is amazing." (Fall 2008)

"Great course. I actually look forward to going to class each lecture. The instructor is very engaging -- by far the best lecturer I've had at CU...The class is tough but I really feel like I am getting a ton of value out of it." (Fall 2008)

"The professor and TAs definitely know the material inside-out and the lectures are excellent and far more educational than other classes I've taken in the CS dept." (Fall 2008)

"...I really enjoyed OS...(undoubtedly) the most challenging course I've taken, but it was the most interesting and I believe will be the most useful." (Fall 2008)

"One of the best courses taken..." (Spring 2008)

"This class was the class I have learned the most from, and has also been the class from which I have gained the most marketable skills I have and have at least indirectly landed me job offers." (Fall 2007)

"I probably learned more in this course than my last three CS courses combined." (Fall 2007)

"Prof. Nieh is the greatest teacher I ever met." (Fall 2004)

"Best CS teacher at Columbia hands down." (Fall 2004)

"The best lecturer I have ever." (Fall 2004)

"The best one (course) I have ever taken..." (Fall 2004)

"Amazing class and teacher." (Fall 2004)

"Brilliant, knowledgeable, approachable professor." (Fall 2004)

"There's nothing he can't do." (Fall 2004)

"Outstanding professor. Knows EVERYTHING about linux and operating systems in general." (Fall 2004)

"...definitely recommended for any Computer Science student." (Fall 2004)

“Dr. Nieh took a potentially dry topic and made it very interesting. The classroom was very crowded throughout the semester: not just because there were way too many desks and not enough space, but because Dr. Nieh made lectures intriguing enough that most students always came.” (Fall 2004)

“Dr. Nieh is a great professor. I took an Operating Systems course at my undergrad university, and it was very dry. Dr. Nieh made the lectures interesting, and he kept our attention...” (Fall 2004)

“One of the best! If we had more professors like this one, the MS would be number 1!” (Fall 2004)

“I rate this one of the best courses in Columbia University.” (Fall 2004)

“...a fun and highly informative class!” (Fall 2004)

“...my favorite. Being able to hack the Linux kernel is awesome. I am learning a lot. And Professor Nieh’s delivery is second to none...I really do love the course.” (Fall 2004)

“...extremely well organized and handled, despite having a huge number of students.” (Fall 2004)

“Best teacher I have had so far.” (Fall 2003)

“Great teacher, great course. Extremely clear about why things are how they are. Challenges the students to think through the answer instead of just stating it, which too few professors in CS do.” (Fall 2003)

“...a master in his field...a brilliant orator, presenter and well a learned man all in one.” (Fall 2003)

“Professor Nieh runs a class that is orders of magnitude more organized and more thoughtfully planned. He’s structured unbelievably dense material extremely well so that I’m able to follow the course of the subject easily.” (Fall 2003)

“The course material was invaluable. The skills and knowledge you learn are immense.” (Fall 2003)

“...the most enjoyable, informative, and well-structured course...every CS student at Columbia should not miss out the opportunity to learn under him.” (Fall 2003)

“Best lecturer in Computer Science in my academic career.” (Fall 2003)

“The best CS class I’ve had, combines very well theory and practice.” (Fall 2003)

“I recommend more in-depth classes on operating systems to be taught by Prof. Nieh.” (Fall 2003)

“Professor Nieh clearly knows his stuff about OS and is able to teach it to his students very well.” (Fall 2003)

“Very organized, approachable, unlike some professors, knows his stuff very very well. Overall, an awesome professor.” (Fall 2003)

“Professor Nieh is very approachable and extremely knowledgeable. He exudes everything that a teacher should be.” (Fall 2003)

“Knows the subject inside out...very approachable and friendly...strives to provide a quality class, makes no compromises.” (Fall 2003)

“...knows his subject so well...amongst the best professors I have met.” (Fall 2003)

“...very well-lectured and well-run, and I was impressed by the amount that we learned.” (Fall 2003)

“...a very good professor who knows how to relate a difficult subject in a very easy to understand manner.” (Fall 2003)

“Great teacher...you’ll get a lot out from this class, in terms of programming skills and systems knowledge in general...definitely one of the best CS classes I took at Columbia.” (Spring 2003)

“Nieh is an awesome teacher that is very organized and that instructs his class with a lot of thought behind everything.” (Spring 2003)

“Nieh is clear, concise, and eminently knowledgeable within the contemporary operating systems field.” (Spring 2003)

“The best CS professor I have taken a class with.” (Spring 2003)

“Prof. Nieh is very friendly, very knowledgeable in his field and very open to students.” (Spring 2003)

“A tremendous amount of thought was clearly put into the course design. One of the best organized classes I’ve been in.” (Spring 2003)

“Professor Nieh is a great and very knowledgeable professor. He is also always available and willing to help.” (Spring 2003)

"Best organized class I've taken so far. Professor Nieh really cares about what people learn, and he takes his job seriously." (Spring 2003)

"I'm really impressed...never had a course like this..." (Spring 2003)

"Prof. Nieh is an excellent teacher. He is always prepared for class. He maintains an outstanding course website. He also addresses student questions and allows them to think in the classroom... he is very approachable and is a really nice guy...you also gain a lot from the class." (Spring 2003)

"Nieh is a terrific instructor. He has a gift for selecting just the right details to demonstrate a particular point so that the rest of the material falls into place..." (Fall 2002)

"I have not come across a professor as good as he is in my life." (Fall 2002)

"Professor Nieh takes what is possibly the most difficult topic in Computer Science and explains it in a way that makes difficult topics seem almost common-sense. His classroom delivery is impeccable, and the amount learned is incredible." (Fall 2002)

"Nieh is gifted; he has an ability to communicate ideas both colloquially but also with appropriate technical precision." (Fall 2002)

"Aside from knowing his stuff, Prof. Nieh has a great style of lecturing. He always comes prepared, always ready to answer questions, and actually gets you to think about the material." (Fall 2002)

"Great professor, knows his stuff." (Fall 2002)

"Nieh is one of the best professors in the CS department...was always available whether during office hours or not. Compared to other professors, he is a much better speaker and has better presentation skills. His knowledge of subject matter is on par with other great professors I've had. Most importantly, he's a nice and understanding guy which is very welcome in a department of professors who seem like they're out to get you. I learned a tremendous amount and thoroughly enjoyed the class." (Fall 2002)

"A very good instructor in all the sense of the word. He knows his material, listens to students, and is willing to help the students." (Fall 2002)

"...made the Linux kernel accessible to students to a degree I wouldn't have imagined possible." (Fall 2002)

"It's a great, great class." (Fall 2002)

"Very, very knowledgeable and easily approachable." (Fall 2002)

"Highly recommended..." (Spring 2002)

"This class was fun. It's laid back and very instructive..." (Spring 2002)

"This is an excellent class." (Spring 2002)

"Prof. Nieh is by far the best professor I have encountered in this school." (Fall 2001)

"Must-take class for all CS majors." (Fall 2001)

"The best CS class of my college career, both in terms of how much I learned and how valuable the information turned out to be in the real world. Writing new system calls, device drivers, schedulers... Mention to an interviewer that you know how to do this and they drool..." (Fall 2000)

"Hardest, but best class I've taken so far at Columbia..." (Fall 2000)

"This is the best course I have taken in 6 years at the CS dept." (Spring 2000)

"I love that we're working with a real OS like Linux. Doing the homework was fun, particularly so because it felt like really accomplishing something of practical value." (Fall 1999)

"A relative new-comer to Columbia, Nieh is a VERY smart guy, and when it comes to OS, he is THE specialist. His lectures are one of the better ones here at Columbia, and you'll actually learn a lot." (Fall 1999)

"A great course, I really enjoyed it. Thanks." (Spring 1999)

"Best course I've taken at Columbia thus far." (Spring 1999)

Electronic Acknowledgement Receipt

EFS ID:	7444671
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0090
Receipt Date:	19-APR-2010
Filing Date:	08-DEC-2009
Time Stamp:	19:40:05
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Nieh_Declaration.pdf	1488660 39f74042d0fcc15599d3b66aa6721cf03e5a0ec8	no	45

Warnings:

Information:

2	Reexam Certificate of Service	Cert_Serv_Nieh.pdf	24155 2834a429e9606e2234d7163c061a5f3be2978427	no	1

Warnings:

Information:

Total Files Size (in bytes):	1512815

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

EXHIBIT E

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VirnetX Inc.,	§	
	§	
Plaintiff,	§	
	§	
v.	§	
	§	**CIVIL ACTION NO. 6:10-CV-417 LED**
Cisco Systems, Inc.	§	
Apple Inc.	§	**Judge: Hon. Leonard Davis**
Aastra USA Inc.	§	
Aastra Technologies Ltd.	§	
NEC Corporation, and	§	
NEC Corporation of America,	§	
	§	
Defendants.	§	
	§	

DEFENDANT AND COUNTERCLAIM-PLAINTIFF AASTRA USA INC.'S ANSWER, AFFIRMATIVE DEFENSES AND COUNTERCLAIMS TO VIRNETX INC.'S ORIGINAL COMPLAINT

Aastra USA Inc. ("Aastra USA"), defendant and counterclaim-plaintiff in the above-entitled and numbered civil action, replies to the Original Complaint of VirnetX Inc. ("VirnetX") as follows.

THE PARTIES

1. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is "a corporation organized and existing under the laws of the State of Delaware, and maintains its principal place of business at 5615 Scotts Valley Drive, Suite 110 Scotts Valley, California," and, therefore, denies these allegations.

2. Aastra USA admits that Aastra Technologies Limited is a Canadian corporation with its principal place of business at 155 Snow Blvd., Concord, Ontario Canada, L4K 4N9. Aastra USA admits that it is a Delaware corporation with its principal place of business at 2811 Internet Blvd., Frisco, Texas 75034. Aastra USA denies that Aastra Technologies Limited regularly conducts and transacts business in Texas, throughout the United States, and within the Eastern District of Texas. Aastra USA admits that it regularly conducts and transacts business in Texas, throughout the United States, and within the Eastern District of Texas. Aastra USA denies that either it or Aastra Technologies Limited have committed or continues to commit any acts that give rise to any cause of action asserted in VirnetX's complaint. Except as admitted above, Aastra USA denies the allegations of Paragraph 2.

3. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 3 and therefore, denies these allegations.

4. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 4 and therefore, denies these allegations.

5. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 5 and therefore, denies these allegations.

JURISDICTION AND VENUE

6. Aastra USA admits that VirnetX purports to bring this action under the patent laws of the United States, Title 35, United States Code, but Aastra USA denies

any liability thereunder. Aastra USA does not contest that the Court has exclusive subject matter over this matter under 28 U.S.C. § 1338. Except as admitted above, Aastra USA denies the allegations of Paragraph 6.

7. Admitted.

8. Aastra USA admits that this Court has personal jurisdiction over Aastra USA. Except as admitted above, Aastra USA denies the allegations of Paragraph 8.

ASSERTED PATENTS

9. Aastra USA admits that United States Patent No. 6,502,135 ("the '135 patent"), entitled "Agile Network Protocol for Secure Communications with Assured System Availability" issued on December 31, 2002, but denies any further characterization of the '135 patent, its inventors, or its examination as alleged in Paragraph 9. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the "owner of all rights, title, and interest in and to the '135 patent and possesses all rights of recovery under the '135 patent" and, therefore, denies these allegations. Aastra USA admits that a purported copy of the '135 patent was attached to the complaint as Exhibit A. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 9.

10. Aastra USA admits that United States Patent No. 6,839,759 ("the '759 patent"), entitled "Method for Establishing Secure Communication Link Between Computers of Virtual Private Network Without User Entering Any Cryptographic Information" issued on January 4, 2005, but denies any further characterization of the '759 patent, its inventors, or its examination as alleged in Paragraph 10. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the

allegations that VirnetX is the "owner of all rights, title, and interest in and to the '759 patent and possesses all rights of recovery under the '759 patent" and, therefore, denies these allegations. Aastra USA admits that a purported copy of the '759 patent was attached to the complaint as Exhibit B. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 10.

11. Aastra USA admits that United States Patent No. 7,188,180 ("the '180 patent"), entitled "Method for Establishing Secure Communications Link Between Computers of Virtual Private Network" issued on March 6, 2007, but denies any further characterization of the '180 patent, its inventors, or its examination as alleged in Paragraph 11. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the "owner of all rights, title, and interest in and to the '180 patent and possesses all rights of recovery under the '180 patent" and, therefore, denies these allegations. Aastra USA admits that a purported copy of the '180 patent was attached to the complaint as Exhibit C. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 11.

12. Aastra USA admits that United States Patent No. 7,418,504 ("the '504 patent"), entitled "Agile Network Protocol for Secure Communications Using Secure Domain Names" issued on August 26, 2008, but denies any further characterization of the '504 patent, its inventors, or its examination as alleged in Paragraph 12. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the "owner of all rights, title, and interest in and to the '504 patent and possesses all rights of recovery under the '504 patent" and, therefore, denies these allegations. Aastra USA admits that a purported copy of the '504 patent

was attached to the complaint as Exhibit D. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 12.

13. Aastra USA admits that United States Patent No. 7,490,151 ("the '151 patent"), entitled "Establishment of a Secure Communication Link Based on a Domain Name Service (DNS) Request" issued on February 10, 2009, but denies any further characterization of the '151 patent, its inventors, or its examination as alleged in Paragraph 13. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the "owner of all rights, title, and interest in and to the '151 patent and possesses all rights of recovery under the '151 patent" and, therefore, denies these allegations. Aastra USA admits that a purported copy of the '151 patent was attached to the complaint as exhibit E. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 13.

COUNT ONE

PATENT INFRINGEMENT BY AASTRA USA

14. Aastra USA incorporates by reference paragraphs 1-13 as if fully set forth herein. Aastra USA denies that it has infringed and/or continues to infringe the '135 patent.

15. Aastra USA admits that it makes, sells, offers for sale, exports, imports, supplies, and/or distributes within and from the United States the Clearspan platform, Pointspan platform, 6725ip telephone, 6721ip telephone, 6739i telephone, 6730i telephone, 6731i telephone, 6753i (53i) telephone, 6755i (55i) telephone, 6757i (57i) telephone, 6757i CT (57i CT) telephone, M670i (536M) Expansion Module, M675i (560M) Expansion Module, 9143i telephone, 9480i telephone, and 9480i CT

telephone. Aastra USA denies that any of these products infringe any valid claim of the '135 patent. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 15.

16. Aastra USA admits that it uses the products listed in Paragraph 15, but denies that such use infringes any valid claim of the '135 patent. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 16.

17. Aastra USA admits that it sells the products listed in Paragraph 15 to parties who use said products, but denies that such use infringes any valid claim of the '135 patent. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 17.

18. Denied.

19. Denied.

20. Denied.

21. Denied.

22. Aastra USA admits that it has received actual notice of infringement by virtue of the filing of this lawsuit. Aastra USA denies that it has received constructive notice. Aastra USA denies that VirnetX has complied with the requirements of 35 U.S.C. § 287. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 22.

COUNT TWO

PATENT INFRINGEMENT BY APPLE

23. Aastra USA incorporates by reference paragraphs 1-22 as if fully set forth herein. Aastra USA is without knowledge or information sufficient to form a belief as

to the truth of the allegations set forth in Paragraph 23 and therefore, denies these allegations.

24. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 24 and therefore, denies these allegations.

25. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 25 and therefore, denies these allegations.

26. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 26 and therefore, denies these allegations.

27. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 27 and therefore, denies these allegations.

28. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 28 and therefore, denies these allegations.

29. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 29 and therefore, denies these allegations.

30. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 30 and therefore, denies these allegations.

31. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 31 and therefore, denies these allegations.

32. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 32 and therefore, denies these allegations.

33. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 33 and therefore, denies these allegations.

34. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 34 and therefore, denies these allegations.

35. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 35 and therefore, denies these allegations.

36. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 36 and therefore, denies these allegations.

COUNT THREE

PATENT INFRINGEMENT BY CISCO

37. Aastra USA incorporates by reference paragraphs 1-36 as if fully set forth herein. Aastra USA is without knowledge or information sufficient to form a belief as

to the truth of the allegations set forth in Paragraph 37 and therefore, denies these allegations.

38. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 38 and therefore, denies these allegations.

39. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 39 and therefore, denies these allegations.

40. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 40 and therefore, denies these allegations.

41. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 41 and therefore, denies these allegations.

42. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 42 and therefore, denies these allegations.

43. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 43 and therefore, denies these allegations.

44. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 44 and therefore, denies these allegations.

45. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 45 and therefore, denies these allegations.

46. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 46 and therefore, denies these allegations.

47. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 47 and therefore, denies these allegations.

48. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 48 and therefore, denies these allegations.

49. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 49 and therefore, denies these allegations.

50. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 50 and therefore, denies these allegations.

51. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 51 and therefore, denies these allegations.

52. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 52 and therefore, denies these allegations.

53. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 53 and therefore, denies these allegations.

54. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 54 and therefore, denies these allegations.

55. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 55 and therefore, denies these allegations.

56. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 56 and therefore, denies these allegations.

57. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 57 and therefore, denies these allegations.

58. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 58 and therefore, denies these allegations.

59. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 59 and therefore, denies these allegations.

60. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 60 and therefore, denies these allegations.

61. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 61 and therefore, denies these allegations.

62. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 62 and therefore, denies these allegations.

63. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 63 and therefore, denies these allegations.

COUNT FOUR

PATENT INFRINGEMENT BY NEC

64. Aastra USA incorporates by reference paragraphs 1-63 as if fully set forth herein. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 64 and therefore, denies these allegations.

65. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 65 and therefore, denies these allegations.

66. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 66 and therefore, denies these allegations.

67. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 67 and therefore, denies these allegations.

68. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 68 and therefore, denies these allegations.

69. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 69 and therefore, denies these allegations.

70. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 70 and therefore, denies these allegations.

71. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 71 and therefore, denies these allegations.

72. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 72 and therefore, denies these allegations.

73. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 73 and therefore, denies these allegations.

74. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 74 and therefore, denies these allegations.

75. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 75 and therefore, denies these allegations.

76. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 76 and therefore, denies these allegations.

77. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 77 and therefore, denies these allegations.

AASTRA USA'S AFFIRMATIVE DEFENSES

78. Aastra USA has not and does not literally, directly, contributorily, by way of inducement, and/or under the doctrine of equivalents, infringe any valid and/or enforceable claim of the '135 patent.

79. Each of the claims of the '135 patent are invalid for failing to comply with one of more of the requirements for patentability specified by Part II of Title 35 of the United States Code §101 *et seq.*, including without limitation 35 U.S.C. §§ 102, 103 and/or 112.

80. VirnetX is estopped from construing the claims of the '135 patent to cover or include, either literally or by application of the doctrine of equivalents, methods used, devices manufactured, used, imported, sold or offered for sale by Aastra USA because of admissions and statements to the PTO during prosecution of the applications leading to the issuance of the patent, disclosure or language in the specification of the patent and/or limitations in the claims of the patent.

81. The relief sought by VirnetX is barred in whole or in part by the doctrine of laches.

82. To the extent that products accused of infringement were or are used or manufactured by or for the United States , the relief sought by VirnetX is limited by 28 U.S.C. § 1498(a).

83. The relief sought by VirnetX is barred in whole or in part by 35 U.S.C. § 287.

84. VirnetX is not entitled to an injunction against Aastra USA because VirnetX has an adequate remedy at law.

85. VirnetX lacks standing to bring suit to enforce the '135 patent because it does not possess all substantial rights in the '135 patent.

86. The '135 patent is unenforceable due to inequitable conduct. Based on the contents of the prosecution history and based on Aastra USA's understanding of the

allegations by VirnetX, one or more of the people substantively involved in the prosecution of the application leading to the '135 patent, and the subsequent reexamination of the '135 patent, were aware of information material to the patentability of the claims of the '135 patent, but withheld that information from the Patent Office with the intent to deceive.

Existence of US. Patent Application No. 09/399,753 ("the Miller Application"), was withheld during the prosecution of the '135 patent. The pendency of the Miller Application was information material to patentability of the '135 patent based on Aastra USA's understanding of the allegations by VirnetX. The withheld information also includes RFC 2401-Security Architecture for the Internet Protocol ("RFC 2401") and the Aventail Administrator's Guide ("Aventail"), which are material to patentability based upon Aastra USA's understanding of the allegations by VirnetX. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

The Miller Application, RFC 2401, and the Aventail reference are not cumulative to the prior art made of record during prosecution of the '135 patent. There is a substantial likelihood that a reasonable examiner would have considered this art in determining whether to allow the '135 patent to issue.

During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution (including Ross Dannenburg) were aware of the Miller Application. Mr. Dannenburg was involved in the prosecution of the Miller Application during the prosecution of the '135 patent at least as early as June 14, 2002, when he signed an Amendment / Response in the prosecution history of the Miller Application. Mr. Dannenburg was involved in the prosecution of the '135 patent at least as early as January 28, 2002, when he signed a Transmittal Form for an Amendment / Response in the prosecution file history of the '135 patent. Therefore, Mr. Dannenburg was involved in the prosecution of the Miller Application while he was prosecuting the '135 patent. Based on Aastra USA's understanding of the allegations by VirnetX, the pendency of the Miller Application is information material to patentability. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to disclose this material information to the Patent Office at any time during the prosecution of the '135 patent with intent to deceive. Moreover, the materiality of the Miller Application leads to an inference of intent to deceive. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution were aware of RFC 2401, including Mr. Dannenburg, because it is mentioned in the specification of the '135 patent. Based on Aastra USA's understanding of the allegations by VirnetX, RFC 2401 is material prior art. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to submit this material prior art reference to the Patent Office as required by 37 C.F.R. 1.56 and 37 C.F.R. 1.97, with intent to deceive. Moreover, in mentioning RFC 2401 in the application, those substantively involved in the prosecution of the application described RFC 2401 in a way that concealed its materiality, with intent to deceive. Moreover, the materiality of

RFC 2401 leads to an inference of intent to deceive. This conduct, undertaken with the intent to deceive the Patent Office, constitutes inequitable conduct.

VirnetX also committed inequitable conduct during the reexamination of the ‘135 patent. On or about February 15, 2007, VirnetX filed a lawsuit against Microsoft Corporation (“Microsoft”) in the Eastern District of Texas, Tyler Division, C.A. No. 6:07-CV-80 (the “Microsoft trial”), alleging that Microsoft infringed certain VirnetX patents, including the ‘135 patent.

During the Microsoft trial, one or more witnesses for VirnetX, including inventor Edward Munger, testified that the claims of the ‘135 patent were conceived no earlier than three months after September 23, 1999, placing the date of conception for claims 1-10 and 12 on or after December 23, 1999.

During the Microsoft trial, Microsoft alleged, in part, that claims 1-10 and 12 of the ‘135 patent were anticipated by the Aventail reference, which on information and belief bears a copyright date between 1996 – 1999.

In December 2009, Microsoft filed a reexamination request with the Patent Office requesting re-examination of claims 1-10 and 12 of the ‘135 patent, citing, among other references, the Aventail reference as prior art under 35 U.S.C. § 102(a). Microsoft asserted that the Aventail reference anticipated claims 1-10 and 12 of the ‘135 patent.

On or about December 31, 2009, the Patent Office ordered re-examination of claims 1-10 and 12 of the ‘135 patent, finding, in part, that the Aventail reference raised a substantial new question of patentability of all of the requested claims of the ‘135 patent.

On or about January 15, 2010, the Patent Office issued a non-final action rejecting claims 1, 3, 4, 6-10, and 12 as being anticipated by the Aventail reference.

On or about February 22, 2010, VirnetX filed a petition to extend its deadline for responding to the office action, pointing out, in part, that it needed additional time to investigate whether the Aventail reference was proper prior art, including investigating the dates of conception and reduction to practice of the inventions claimed in the '135 patent as well as diligence there between. The petition also cited as a basis for extension that the Microsoft case was causing a "significant drain" on VirnetX's resources. Moreover, the petition stated that the extension "would likely also permit consideration of any court conclusions regarding the claims presently under reexamination." The petition was filed by Toby Kusmer of McDermott Will & Emery, the same firm that represented VirnetX in the Microsoft case until 2009. The Patent Office responded on or about February 24, 2010, granting an extension, and setting the deadline for response as April 15, 2010.

On or about March 8, 2010, the Microsoft trial commenced. During trial, Microsoft argued that the Aventail reference invalidated claims 1-10 and 12 of the '135 patent. Microsoft presented evidence indicating that the Aventail reference may have been published as early as June 1999. Based on a review of the trial record, VirnetX did not dispute the publication date of the Aventail reference. The Microsoft trial concluded on or about March 16, 2010. Therefore, at least as of March 16, VirnetX was aware that the Aventail reference may have been published at least as early as June 1999, which is prior to the February 15, 2000, filing date of the application that matured into the '135 patent and prior to the earliest conception date of December 1999 claimed by the inventor of the '135 patent.

On or about March 25, 2010 VirnetX gave notice to the Patent Office of the outcome of the case and submitted the jury verdict form from the case. On or about March 29, 2010, VirnetX filed a petition requesting that the re-examination proceeding be suspended. The Patent Office did not respond to the request until after the date set for VirnetX's response to the non-final office action rejection.

On or about April 15, 2010, VirnetX responded to the office action rejection, in part, by asserting that the Aventail reference should not be considered prior art because no evidence had been submitted by Microsoft that established the actual publication date of the Aventail reference. Moreover, VirnetX did not provide the result of any investigation it may have made with respect to the publication date of the Aventail reference or the dates of conception or reduction to practice of the '135 patent that it indicated it would make in its petition for an extension of time, nor did VirnetX provide any information that it learned from the Microsoft trial that related to the publication date of the Aventail reference. Based on a review of the prosecution history, VirnetX did not disclose that its conception date for the claims of the '135 patent was no earlier than December 1999, nor did VirnetX disclose that the Aventail reference may have been published as early as June 1999, a fact to which VirnetX was made aware during the Microsoft trial.

On June 16, 2010, the Patent Office issued an Action Closing Prosecution. In the action, the examiner recites that he made an attempt to determine the publication date of the Aventail reference, but was unsuccessful. Based on the lack of evidence of the publication date, the examiner withdrew all of the rejections that had been based on the Aventail reference.

VirnetX and/or its representatives, agents, and attorneys who were substantively involved in the prosecution of the re-examination knew or should have known of the Microsoft trial and the evidence presented regarding the publication date of the Aventail reference. For example, Mr. Kusmer specifically referenced the Microsoft trial and the potential for additional material information to come to light during that trial when seeking an extension to respond to an office action, as set forth above. VirnetX and/or its representatives, agents, and attorneys withheld this information with the intent to deceive, either willfully or with such gross negligence or recklessness as constituting an act of willfulness amounting to inequitable conduct. Moreover, the high degree of materiality of the Aventail publication and the aforementioned evidence presented at the Microsoft trial leads to an inference of intent to deceive. Among other things, the information withheld was material to the reexamination of the '135 patent, in violation of the duty of candor the representatives and/or the attorneys owed to the Patent Office.

AASTRA USA'S COUNTERCLAIMS

87. Aastra USA Inc. ("Aastra USA") is a Delaware corporation with its principal place of business at 2811 Internet Blvd., Frisco, Texas 75034.

88. VirnetX, Inc. ("VirnetX"), as represented in Paragraph 1 of its Original Complaint, has claimed that it is a Delaware corporation with its principal place of business at 5615 Scotts Valley Drive, Suite 110 Scotts Valley, California.

89. This Court has subject matter jurisdiction over the Counterclaim pursuant to 28 U.S.C. §§ 1331, 1338, and 2201 as it arises under an Act of Congress relating to patents.

90. Venue is proper in this district under 28 U.S.C. §§ 1391(b), (c) and 1400.

91. By filing its complaint, VirnetX has consented to the personal jurisdiction of this Court.

DECLARATORY JUDGMENT FOR NON-INFRINGEMENT OF UNITED STATES PATENT NO. 6,502,135

92. Aastra USA hereby re-alleges and incorporates by reference Paragraphs 87-91 as though fully set forth herein.

93. United States Patent No. 6,502,135 ("the '135 patent"), entitled "Agile Network Protocol for Secure Communications with Assured System Availability" was issued on December 31, 2002. VirnetX claims to be the owner by assignment of the '135 patent.

94. Aastra USA has not directly infringed, contributed to infringement, or induced infringement of any valid claim of the '135 patent, nor is Aastra USA directly infringing, contributing to infringement, or inducing infringement of any valid claim of the '135 patent.

95. An actual controversy exists between Aastra USA and VirnetX regarding the alleged infringement '135 patent by virtue of VirnetX's allegation of infringement.

96. Aastra USA is entitled to judgment from this Court that the '135 patent is not infringed by Aastra USA.

DECLARATORY JUDGMENT FOR INVALIDITY OF UNITED STATES PATENT NO. 6,502,135

97. Aastra USA hereby re-alleges and incorporates by reference Paragraphs 87-96 as though fully set forth herein.

98. The '135 patent is invalid for failing to comply with one or more of the requirements for patentability set forth in Part II of Title 35 U.S.C. § 101 *et seq.*, including without limitation 35 U.S.C. §§102, 103 and/or 112.

99. An actual controversy exists between Aastra USA and VirnetX regarding the validity of the '135 patent by virtue of VirnetX's allegation of infringement.

100. Aastra USA is entitled to judgment from this Court that the '135 patent is invalid.

DECLARATORY JUDGMENT FOR UNENFORCEABILITY OF UNITED STATES PATENT NO. 6,502,135

101. Aastra USA hereby re-alleges and incorporates by reference Paragraphs 87-100 as though fully set forth herein.

102. The '135 patent is unenforceable due to inequitable conduct. Based on the contents of the prosecution history and based on Aastra USA's understanding of the allegations by VirnetX, one or more of the people substantively involved in the prosecution of the application leading to the '135 patent, and the subsequent reexamination of the '135 patent, were aware of information material to the patentability of the claims of the '135 patent, but withheld that information from the Patent Office with the intent to deceive.

103. The existence of US. Patent Application No. 09/399,753 ("the Miller Application"), was withheld during the prosecution of the '135 patent. The pendency

of the Miller Application was information material to patentability of the ‘135 patent based on Aastra USA’s understanding of the allegations by VirnetX. The withheld information also includes RFC 2401-Security Architecture for the Internet Protocol ("RFC 2401") and the Aventail Administrator’s Guide (“Aventail”), which are material to patentability based upon Aastra USA’s understanding of the allegations by VirnetX. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

104. The Miller Application, RFC 2401, and the Aventail reference are not cumulative to the prior art made of record during prosecution of the ‘135 patent. There is a substantial likelihood that a reasonable examiner would have considered this art in determining whether to allow the ‘135 patent to issue.

105. During the prosecution of the application leading to the ‘135 patent, one or more of the people substantively involved in its prosecution (including Ross Dannenburg) were aware of the Miller Application. Mr. Dannenburg was involved in the prosecution of the Miller Application during the prosecution of the ‘135 patent at least as early as June 14, 2002, when he signed an Amendment / Response in the prosecution history of the Miller Application. Mr. Dannenburg was involved in the prosecution of the ‘135 patent at least as early as January 28, 2002, when he signed a Transmittal Form for an Amendment / Response in the prosecution file history of the ‘135 patent. Therefore, Mr. Dannenburg was involved in the prosecution of the Miller Application while he was prosecuting the ‘135 patent. Based on Aastra USA’s understanding of the allegations by VirnetX, the pendency of the Miller Application is information material to patentability. Nonetheless, those substantively involved in

the prosecution of the application intentionally failed to disclose this material information to the Patent Office at any time during the prosecution of the '135 patent with intent to deceive. Moreover, the materiality of the Miller Application leads to an inference of intent to deceive. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

106. During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution were aware of RFC 2401, including Mr. Dannenburg, because it is mentioned in the specification of the '135 patent. Based on Aastra USA's understanding of the allegations by VirnetX, RFC 2401 is material prior art. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to submit this material prior art reference to the Patent Office as required by 37 C.F.R. 1.56 and 37 C.F.R. 1.97, with intent to deceive. Moreover, in mentioning RFC 2401 in the application, those substantively involved in the prosecution of the application described RFC 2401 in a way that concealed its materiality, with intent to deceive. Moreover, the materiality of RFC 2401 leads to an inference of intent to deceive. This conduct, undertaken with the intent to deceive the Patent Office, constitutes inequitable conduct.

107. VirnetX also committed inequitable conduct during the reexamination of the '135 patent. On or about February 15, 2007, VirnetX filed a lawsuit against Microsoft Corporation ("Microsoft") in the Eastern District of Texas, Tyler Division, C.A. No. 6:07-CV-80 (the "Microsoft trial"), alleging that Microsoft infringed certain VirnetX patents, including the '135 patent.

108. During the Microsoft trial, one or more witnesses for VirnetX, including inventor Edward Munger, testified that the claims of the '135 patent were conceived no earlier than three months after September 23, 1999, placing the date of conception for claims 1-10 and 12 on or after December 23, 1999.

109. During the Microsoft trial, Microsoft alleged, in part, that claims 1-10 and 12 of the '135 patent were anticipated by the Aventail reference, which on information and belief bears a copyright date between 1996 – 1999.

110. In December 2009, Microsoft filed a reexamination request with the Patent Office requesting re-examination of claims 1-10 and 12 of the '135 patent, citing, among other references, the Aventail reference as prior art under 35 U.S.C. § 102(a). Microsoft asserted that the Aventail reference anticipated claims 1-10 and 12 of the '135 patent.

111. On or about December 31, 2009, the Patent Office ordered re-examination of claims 1-10 and 12 of the '135 patent, finding, in part, that the Aventail reference raised a substantial new question of patentability of all of the requested claims of the '135 patent.

112. On or about January 15, 2010, the Patent Office issued a non-final action rejecting claims 1, 3, 4, 6-10, and 12 as being anticipated by the Aventail reference.

113. On or about February 22, 2010, VirnetX filed a petition to extend its deadline for responding to the office action, pointing out, in part, that it needed additional time to investigate whether the Aventail reference was proper prior art, including investigating the dates of conception and reduction to practice of the inventions claimed in the '135 patent as well as diligence there between. The petition

also cited as a basis for extension that the Microsoft case was causing a "significant drain" on VirnetX's resources. Moreover, the petition stated that the extension "would likely also permit consideration of any court conclusions regarding the claims presently under reexamination." The petition was filed by Toby Kusmer of McDermott Will & Emery, the same firm that represented VirnetX in the Microsoft case until 2009. The Patent Office responded on or about February 24, 2010, granting an extension, and setting the deadline for response as April 15, 2010.

114. On or about March 8, 2010, the Microsoft trial commenced. During trial, Microsoft argued that the Aventail reference invalidated claims 1-10 and 12 of the '135 patent. Microsoft presented evidence indicating that the Aventail reference may have been published as early as June 1999. Based on a review of the trial record, VirnetX did not dispute the publication date of the Aventail reference. The Microsoft trial concluded on or about March 16, 2010. Therefore, at least as of March 16, 2010, VirnetX was aware that the Aventail reference may have been published at least as early as June 1999, which is prior to the February 15, 2000, filing date of the application that matured into the '135 patent and prior to the earliest conception date of December 1999 claimed by the inventor of the '135 patent.

115. On or about March 25, 2010, VirnetX gave notice to the Patent Office of the outcome of the case and submitted the jury verdict form from the case. On or about March 29, 2010, VirnetX filed a petition requesting that the re-examination proceeding be suspended. The Patent Office did not respond to the request until after the date set for VirnetX's response to the non-final office action rejection.

116. On or about April 15, 2010, VirnetX responded to the office action rejection, in part, by asserting that the Aventail reference should not be considered prior art because no evidence had been submitted by Microsoft that established the actual publication date of the Aventail reference. Moreover, VirnetX did not provide the result of any investigation it may have made with respect to the publication date of the Aventail reference or the dates of conception or reduction to practice of the '135 patent that it indicated it would make in its petition for an extension of time, nor did VirnetX provide any information that it learned from the Microsoft trial that related to the publication date of the Aventail reference. Based on a review of the prosecution history, VirnetX did not disclose that its conception date for the claims of the '135 patent was no earlier than December 1999, nor did VirnetX disclose that the Aventail reference may have been published as early as June 1999, a fact to which VirnetX was made aware during the Microsoft trial.

117. On June 16, 2010, the Patent Office issued an Action Closing Prosecution. In the action, the examiner recites that he made an attempt to determine the publication date of the Aventail reference, but was unsuccessful. Based on the lack of evidence of the publication date, the examiner withdrew all of the rejections that had been based on the Aventail reference.

118. VirnetX and/or its representatives, agents, and attorneys who were substantively involved in the prosecution of the re-examination knew or should have known of the Microsoft trial and the evidence presented regarding the publication date of the Aventail reference. For example, Mr. Kusmer specifically referenced the Microsoft trial and the potential for additional material information to come to light

during that trial when seeking an extension to respond to an office action, as set forth above. VirnetX and/or its representatives, agents, and attorneys withheld this information with the intent to deceive, either willfully or with such gross negligence or recklessness as constituting an act of willfulness amounting to inequitable conduct. Moreover, the high degree of materiality of the Aventail publication and the aforementioned evidence presented at the Microsoft trial leads to an inference of intent to deceive. Among other things, the information withheld was material to the reexamination of the '135 patent, in violation of the duty of candor the representatives and/or the attorneys owed to the Patent Office.

EXCEPTIONAL CASE

119. This is an exceptional case pursuant to 35 U.S.C. § 285 entitling Aastra USA to an award of attorneys' fees as a result of, *inter alia*, VirnetX's assertion of the '135 patent against Aastra USA with the knowledge that the '135 patent is unenforceable and for VirnetX's failure to perform a reasonable pre-suit investigation of its infringement contentions against Aastra USA.

DEMAND FOR JURY TRIAL

120. Aastra USA hereby demands a jury for all issues so triable.

PRAYER FOR RELIEF

121. WHEREFORE, Aastra USA prays for the following relief:

A. That the Court enter judgment that VirnetX is not entitled to any relief with respect to its allegations against Aastra USA and dismiss all of VirnetX's allegations with prejudice;

B. That the Court enter a judgment that Aastra USA has not infringed and is not directly infringing or indirectly infringing by contribution or inducement, whether willfully or otherwise, any claim of the '135 patent, as alleged by VirnetX;

C. That the Court enter a judgment that the claims of the '135 patent are invalid;

D. That the Court enter a judgment that the claims of the '135 patent are unenforceable;

E. That the Court enter a declaratory judgment that the claims of the '135 patent are not infringed;

F. That the Court enter a declaratory judgment that the claims of the '135 patent are invalid;

G. That the Court enter a declaratory judgment that the claims of the '135 patent are unenforceable;

H. That the Court declare this an exceptional case and award Aastra USA its costs, expenses, and reasonable attorneys' fees pursuant to 35 U.S.C. § 285 and all other applicable statutes, rules, and common law; and

I. That the Court award Aastra USA such other and further relief as the Court may deem just and proper.

DATED: October 29, 2010

Respectfully Submitted,

By: /s/ Phillip N. Cockrell ____
Phillip N. Cockrell
Lead Attorney
State Bar No. 04465500
pcockrell@pattonroberts.com
PATTON ROBERTS, PLLC
400 Century Plaza
2900 St. Michael Dr.
Texarkana, Texas 75503
Telephone: 903-334-7000
Facsimile: 903-334-7007

Jon B. Hyland
jhyland@pattonroberts.com
State Bar No. 24046131
Robert D. Katz
rkatz@pattonroberts.com
State Bar No. 24057936
PATTON ROBERTS, PLLC
901 Main St., Suite 3300
Dallas, Texas 75202
Telephone: 214-580-3826
Facsimile: 903-334-7007

CERTIFICATE OF SERVICE

This is to certify that all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3) on this the 29th. Day of October, 2010.

__/s/ Phillip N. Cockrell_____

EXHIBIT H

Page 1

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VIRNETX INC. AND SCIENCE APPLICATIONS INTERNATIONAL CORP., Plaintiff,

v.

MICROSOFT CORPORATION, Defendant.

Civil Action No. 6:07CV80V(LED)

Videotape Deposition Upon Oral Examination
of
GARY TOMLINSON

Taken at 925 Fourth Avenue, Suite 2900
Seattle, Washington

DATE: Friday, February 27, 2009

REPORTED BY: Ronald L. Cook
CCR, RMR, CRR

Page 2

APPEARANCES

For the Plaintiffs: HONG S. LIN
McDermott Will & Emery
275 Middlefield Road
Suite 100
Menlo Park, California 94025-4004
650.815.7560
hlin@mwe.com
and
CHRISTOPHER D. BRIGHT
McDermott Will & Emery
18191 Von Karman Avenue
Suite 500
Irvine, California 92612
cbright@mwe.com

For the Defendant: THOMAS KING
Weil, Gotshal & Manges
201 Redwood Shores Parkway
Redwood Shores, California 94065
650.802.3210
thomas.king@weil.com

For the SonicWALL, Inc., and the Witness:
LAUREL M.V. BUCKNER
2101 Fourth Avenue
Suite 400
Seattle, Washington 98121
206.438.7367
lbuckner@sonicwall.com

Also Present: CHRISTOPHER STOW, Videographer

Page 3

INDEX

* * *

Page 4

SEATTLE, WASHINGTON; FRIDAY, FEBRUARY 27, 2009
10:08 A.M.
--o0o--

THE VIDEOGRAPHER: Here begins Volume I, Videotape No. 1, in the deposition of Richard Aventail, in the matter of VirnetX, Incorporated, and Science Applications International corporation vs. Microsoft, in the United States District Court for the Eastern District of Texas, Tyler Division, Case No. 6:07CV80V(LED).
Today's date is Friday, February 27, 2009. The time on the video monitor is 10:08 a.m.
The video operator today is Chris Stow, contracted by Merrill Legal Solutions, San Francisco, California.
This video deposition is taking place at 925 Fourth Avenue, Suite 2900, Seattle, Washington, 98104.
Counsel, please identify yourselves and state whom you represent.
MR. KING: Thomas King, from Weil, Gotshal & Manges, here on behalf of Microsoft Corporation.
MR. BRIGHT: Chris Bright, with McDermott Will & Emery, on behalf of plaintiff, VirnetX.
MR. LIN: Hong Lin, also from McDermott Will & Emery, for plaintiff VirnetX.

Page 5

MS. BUCKNER: And I'm Laurel Buckner, associate general counsel at SonicWALL, which was the acquirer of Aventail Corporation, and I'm here primarily to protect SonicWALL's confidential information.
THE VIDEOGRAPHER: The court reporter today is Ronald L. Cook, of Premiere Realtime Litigation Services.
Would the reporter please swear in the witness.

GARY TOMLINSON, deponent herein, being first duly sworn on oath, was examined and testified as follows:

MR. KING: Before we begin the questioning, I'd like to just state -- get -- clarify the record for the record. This is the -- the witness is Gary Tomlinson, and this is a -- he's here representing a company called SonicWALL, Inc.

EXAMINATION

BY MR. KING:
Q. Good morning, Mr. Tomlinson.
A. Good morning.
Q. You understand that you're here to testify

Page 6

today on behalf of SonicWALL, Incorporated; is that --
A. I do.
Q. -- is that correct?
Before we -- before we begin with the deposition, I just want to set a few -- few ground rules. Because you're represented by counsel, I presume you're somewhat familiar with this process, but the way this is going to work today is I'll be asking some questions and you'll be answering those questions to the best of your ability. Is that fair?
A. Yes.
Q. At some point during the process either your counsel or counsel for VirnetX might interpose some objections. That's just for the record, and you understand that you're still under an obligation to answer those questions unless -- unless your counsel directs otherwise; is that fair?
A. Yes, I understand that, mm-hmm.
Q. And the last thing, and this is hard, but -- as the day goes on, but for the sake of the court reporter, let's try to just have one person talking at a time so we can have a clear record. Is that fair?
A. Yes.
Q. Is there any reason why you can't give full and -- full and truthful testimony today?

Page 7

A. No, there's no reason.
MR. KING: Let's see. I'd like to mark an exhibit.
(Discussion off the record.)
(Deposition Exhibit 1 was marked for identification.)
Q. BY MR. KING: Have you ever seen this document before?
A. Let me look.
I'm not sure if I've seen this. I think I have but I'm not sure. I've seen several documents presented to us.
Q. Okay.
I'll represent to you that is the subpoena that we sent SonicWALL, requesting production of documents and requesting that someone from -- a representative from SonicWALL come to testify about a partic -- some topics.
Would you mind turning to Page 6?
A. Sure.
Q. It's Page 6 of Attachment A.
A. Of Attachment --
Q. Or might also be --
A. It says "Attachment B."
Q. It's labeled "Attachment B." Okay.
A. Is that --

Page 8

Q. That's it.
A. Okay.
Q. Do you see up at the top where it says "Deposition Topics"?
A. Yes.
Q. Have you seen -- have you seen this page before?
A. I believe so. It's been some time since I've seen it.
Q. All right.
Are you prepared to testify on these topics today?
A. Yeah, to my best of my ability, yes.
Q. Okay.
Before we do that, I'd like to take a few minutes and walk through -- walk through your background, your -- starting with your education. Would you please tell me where you went to school after -- after high school?
A. I went to two schools. I went to Antelope Valley Community College, where I picked up an Associate's of Science degree on my way to a four-year degree, and then I matriculated into California State University at Northridge, where I picked up a Bachelor of Science in business administration, information systems.
Q. And what -- what year did you graduate from

Page 9

Cal State Northridge?
A. 1979.
Q. Where did you go to -- where did you start working after graduation?
A. I began my career at -- let's see. Sperry Univac was the name at that time, in Salt Lake City, Utah, and I was there four years for my first stint.
Q. And what was your -- what was your position at Sperry Univac?
A. I was a -- a systems developer, so I was brought in and I worked on operating systems and communication subsystems.
Q. What is Sperry Univac's line of business?
A. At that time?
Q. At that time.
A. Primarily -- I mean, it was a -- what would you call it? A large-scale computer systems provider. I worked in mainframes and at that time front-end processors, which were -- you'd think of more like a minicomputer of the era but specialized.
Q. Where did you go after leaving Sperry Univac?
A. I went to a startup that some friends of mine had done, and I -- we were in -- oddly enough, insurance sales support systems. I spent two years there, until the business folded.

Page 10

Q. This was in 1985?
A. Yeah. Yeah, it -- that's right. It folded in 1985.
Q. Where did you go after -- after the -- after your startup folded?
A. I returned to -- to Sperry.
Q. Mm-hmm.
A. And I stayed there until 1989. I went through the Unisys merger.
Q. What was your role during those -- during that time period at Sperry?
A. I was a developer.
Q. Mm-hmm.
A. I -- along the way, in 1982, I started picking up Unix skills at Sperry Univac. I went back because I had extensive Unix background, and I did development of TCP/IP and quite a bit of ARPANET type -- type stuff.
Q. Are you a programmer?
A. Am I a programmer?
Q. Yes.
A. I'm a poor programmer nowadays. At one time I was quite skilled.
Q. What were you doing with -- with TCP/IP?
A. I was developing X.25 interfaces for Millnet.

Page 11

We had contracts with the Department of Army and -- what was it? I guess Air Force. So we were hooking in the underlying communication systems to the IP layer, and then I moved on to doing some more, you know, of the IP kind of expanding the stack out in the Berkeley Unix as well as the System 5 Unix.
Q. So you were -- were you building a TCP/IP stack for Unix?
A. Extending it. So the code that we had came from University of California at Berkeley.
Q. Mm-hmm.
A. So we were extending -- there was in that era considerable work going on in the Department of Defense around options and things that weren't in the standard commercial space.
Q. You mentioned X.25. Can you tell me what that is, very briefly?
A. Oh, it's a packet-switched protocol. I don't know if it -- how much it's used anymore, but it was a wide-area protocol, and the -- at that time the standard communi -- wide-area communications that was available was ARPA 1822, which was the original standard that was -- produced the ARPANET, and the U.S. Government -- or the military didn't want to really use that. It was -- it was a little bit of an oddball standard, right? And so X.25 was

Page 12

an international standard, and they were using that for wide-area communications.
Q. What were some of the extensions to TCP/IP that you -- that you built?
A. In -- specifically, mostly centered in the IP layer. There's an area called IP options, and nowadays it's maybe better documented, although I would say marginally documented in some areas. The DOD had a number of -- and I'm not -- I don't really know what they're used for, I just know how to parse them -- options that they were adding in there that we had to include or pass through. And I -- most of it had to do with cryptography.
Q. Are you familiar with cryptography?
A. Marginally.
Q. Are you familiar with network security?
A. That's a broad topic. Yes, to some extent I am.
Q. When did you start working on -- on network security as a -- as a broad topic?
A. 19 -- well, -- yeah, I'd say probably 1996, in earnest.
Q. Okay.
Now, you mentioned that you were with Sperry through a Unisys merger --
A. Yes.

Page 13

Q. -- in 1989?
A. That merger occurred I believe in 1986, '7. I don't remember exactly. But yes. I was -- I was there until 1989.
Q. When did you leave the combined Sperry Unisys company?
A. September of 1989.
Q. And where did you go?
A. I went to Novell.
Q. How long were you at Novell?
A. 10 years.
Q. Until 1999?
A. Yes.
Q. Okay.
A. Actually, until -- I guess slightly over 10 years -- 2000. Until June of 2000.
Q. What was your -- what were your responsibilities during the time you were at Novell?
A. I was a -- I began as kind of a lead developer, and I developed some of the core NetWare product, and then I moved on to Unix and began doing NetWare work with Unix, both on the client and the server sides, and produced -- we produced some stuff for the next computer for -- for Steve Jobs.
And then I moved on to experimental operating

Page 14

systems in the advanced technologies group, and we produced some sort of operating systems that actually never were -- were commercialized, although variations of them were cut out and commercialized in NetWare. And I was a part of the -- the Unix -- when Novell acquired the Unix labs, I was promoted to a director position. I ran a fairly large engineering team, on the order of about 80 people.
And when I was in the advanced technologies I was kind of a combination individual contributor and I ran the organization from the -- the development side of advanced tech.
I guess -- let's see. What would be interesting?
That's where my security actually began. So it was with respect to Internet security.
So we -- when I was in Novell we produced very, very fast and scalable proxy technology, and to that we added a comprehensive security suite, known as the Border Manager of the era. I believe that was first made available in -- commercially in nineteen ninety -- either seven or eight. I don't recall when it actually came to the street, but it was developed in the '95 to '97 time frame.
And in that we put in virtual private networking technology, both the beginnings of the IPSEC of that era as well as we put SOCKS in. That was kind of an

Page 15

emerging space that -- that people were actually using for some virtual private networks of the day.
And that's -- that's kind of where I began what you would think of as a -- a net -- you know, a network security background, was -- was putting those in. And firewall rules, things like that.
Q. Mm-hmm.
Can you explain more about how Border Manager worked?
A. Sure. Border Manager was a -- a suite of services that ran on the NetWare operating system. The services were -- let's see. There was a basic firewall that would not be a stateful packet firewall, that would be just a strictly rule-based, you know, simple layer 3 and 4 firewall, just kind of ACLs, not really looking at content.
We also had a -- like I said, a SOCKS proxy in there, to do various forms of what we would think as virtual private networks. We had an early-day IPSEC VPN, and we also had a Web proxy, both a forward proxy as well as a reverse proxy, that had access control capabilities, and so that could also be used for a form of security or acceleration and scaling. That was a whole suite of products, known as Border Manager.
And then I went on to a variation of that, which was called Internet Caching System, ICS, and that was

Page 16

OEM to a number of companies. Dell and IBM were the -- the two biggest that come to mind. What we were doing there is the -- the Border Manager was a product that was very NetWare centric so it was kind of to a classic Novell audience and not as -- not as broadly applicable outside the Novell networks. I don't know if you remember the era. Novell was quite large in those days, had somewhere like 90 percent of the market share, so -- anyway, the Border Manager was relatively popular, but, you know, we had a number of ISPs that -- they didn't really want NetWare, they wanted it, quote, to look like a Cisco router, so, you know, we repackaged it into an appliance and kind of took it out the NetWareisms and offered that.
That product was not really a security -- security-oriented product. That was mainly a Internet infrastructure scaling product. So that was more around the Web caches and things like that.
Q. Okay. We'll come back to that one.
Where did you -- where did you go after leaving Novell in 2000?
A. I went to a startup, called Entera, E-n-t-e-r-a, Inc.
Q. And what were your -- what was your job title at Entera, Inc.?
A. I was the chief scientist of Entera.

Page 17

Q. And what were your responsibilities?
A. Designing kind of and managing the -- well, designing new products and managing the technology for the CTO. And our products were in streaming media, so we did stream splitting and caching, and it was very much oriented around scaling streaming media for -- basically for public infrastructure, primarily.
Q. How long were you at Entera?
A. Well, Entera became acquired by CacheFlow, and I moved in to CacheFlow, I was there until April of 2002, and my last role was the CTO of the company.
Q. Mm-hmm.
Was that when you joined Aventail?
MR. LIN: Object to form.
THE WITNESS: What was that?
MR. LIN: I was objecting to form.
THE WITNESS: Objecting?
MR. LIN: Yes.
THE WITNESS: Okay.
MR. KING: Let me just ask a different question, then.
Q. Where did you go after leaving Entera or leaving -- in 2002?
A. Where did I go?
I was doing some independent consulting.

Page 18

Q. Mm-hmm.
A. And I knew the Aventail folks from prior -- from my Novell days. We had done some work with them. And so I -- I had developed a considerable background in kind of the appliance space, Internet appliances, and Aventail was interested in producing such a product. So I took on a consulting role that grew to consuming all of my time. I was a consultant from May 2002 until February 2003, at which point I joined Aventail as their chief architect.
Q. Mm-hmm.
Are you still a chief architect within SonicWALL?
A. No. I am a vice-president of -- of one of the software engineering groups.
Q. Mm-hmm.
A. Primarily the VPN group.
Q. Okay.
What was your -- what were your responsibilities when you joined Aventail in 2003 as a chief architect?
A. I was responsible for bringing essentially the -- the overall architecture of -- of our product lines, you know, kind of bringing them together and driving them forward over time into new products. And additionally, you know, I had to manage some of the teams along the way.

Page 19

Q. What Aventail products were you working with in 2003, when you joined?
A. I worked primarily with -- well, to some extent all of them in my role. My -- my primary area was on the server side, so we -- we already had existing clients that they were in reasonably good shape, but the challenge was we were moving from a managed service -- we had a managed service offering, and we needed to turn that into, you know, the -- an appliance, and that's -- I mean, that's very much around turnkey and kind of op -- you know, there's no humans involved in back rooms and things like hosted services. So a lot of my attention in the early part was on the server, getting that into a suitable form factor for, you know, what -- what customers would consider an appliance that met the operational expense needs.
Then -- in -- so from the very beginning it was mostly taking existing services and straightening them out. That would have been a lot of 2003.
Q. Can you give me the -- some names of Aventail servers that were in existence when you started in 2003?
A. Oh, the services?
Q. Sorry. Servers.
A. Servers.
What do you mean by "server"?
Q. Let's start -- did Aventail sell a VPN server

Page 20

when you joined in 2003?
A. Yes.
Q. What was it called?
A. There were two VPN servers. I -- I tend to call them services. I may have messed you up. I think the term "server" is sometimes overloaded to mean either a particular piece of software on a box or the box.
Q. Mm-hmm.
A. So -- but if you mean a piece of software on the box that provided a service, yes. There were two servers in 2003 that were VPN oriented. One was called the Anywhere VPN Server, AVPN, formerly known as the ExtraNet Server in marketing. The other was the ExtraWeb Server. The Ex -- the AVPN server -- or I guess maybe I should just refer to it as ExtraNet; I think that people know it better by that term -- was a SOCKS-based VPN server, that would handle TCP traffic -- it was, well, tunneled through TCP and SOCKS, it could handle TCP-originated connections from clients, you know, to other systems, and it had some minimal UDP capabilities in it.
The ExtraWeb Server was a reverse Web proxy that would represent basically a whole series of internal Web servers, basically doing rewriting of URLs, right? So everything would be redirected to it, and through URL encoding, right, it would derive the correct destination Web

Page 21

server and then present it through. And that -- that was a Web-only VPN service, as opposed to the AVPN/ExtraNet, which was a -- kind of a general, you know, TCP/IP and limited UDP application VPN.

Q. Now, you mentioned -- you've mentioned SOCKS a couple times. Can you tell me what -- what SOCKS stands for?

A. Oh. You know, I don't remember the exact definition. I mean -- it's an I -- it's an IETF standard, and I -- I don't remember. But it's -- you know, it's a -- it's a way to encapsulate traffic securely through a tunnel.

Q. You mentioned ExtraNet Server a few minutes ago.

A. Yes.

Q. What -- what was Aventail's current version of ExtraNet Server when you joined in 2003?

A. Boy. Hmm.

I'm a little un -- unsure, because we renumbered and named things in 2002. So it -- by then they were all a part of a -- of the -- the new appliance software, which was called ASAP, Aventail Secure Access Platform. And it was using a relatively new version of the SOCKS server that was developed in -- I am not sure when it started, but it -- it came to market for the first time in -- in 2002.

Page 22

Oh, wait. Let me think.

In beta form in 2002, and was released to the public in the spring of 2003. And I don't -- I don't know the number because it was kind of -- became part of ASAP.

Q. We've been talking about the server side of Aventail's products. What about the -- the client side, what was the client -- what was Aventail's VPN client called?

A. Connect proxy.

Q. Mm-hmm.

A. And -- when I came to the company was called Connect proxy. It was also known as AutoSOCKS.

Q. Mm-hmm.

A. From -- from an earlier era. I believe that was the original name that it was marketed -- possibly marketed under. Definitely internally known as AutoSOCKS.

Q. Did it have any other names?

A. Not to my knowledge. The marketing name was Connect proxy.

Q. Are you familiar with Aventail's corporate history?

MR. LIN: Object to form.

I'm going to be objecting periodically so --

THE WITNESS: Sure.

To varying degrees, yes. I first ran into

Page 23

Aventail in 1996, when I was at Novell, and we were working on that Border Manager product that I told you about, and we were building a SOCKS proxy ourself, and so our business development people at Novell had run into Aventail, who was a new startup in 1996, at one of the trade shows. I don't -- I don't recall which. But -- and, of course, Aventail had a SOCKS client, and they also had a SOCKS server that they were, you know, producing. I don't believe it was commercially available yet but, you know, they were -- they were producing it.

And we -- we met them, and we did some joint work with Aven -- with Aventail in 1997, and probably I would imagine 1998, if -- if memory is correct, where we were doing interoperability testing. So our SOCKS server at Novell would -- was interoperable with Aventail's SOCKS client. So I -- I was familiar with -- with that.

And then through the years, probably 1999 -- I moved to Seattle in the end of 1997, and after moving here I -- I spent more time with the Aventail people on working some of the -- you know, some -- some of the ongoing Novell kind of -- you know, as the products -- versions would change and things like that I would sort of work with Aventail people because I was here. I was still with -- I worked for Novell but I was here.

So, you know, I knew a little about, sort of

Page 24

from a technical standpoint, some of the evolution, although not -- not firsthand, from Aventail. I know a considerably greater amount from mid-2002 on.

Q. BY MR. KING: What -- what sort of communications or interactions did you have with Aventail when a new product came out?

A. We -- we talked about, sort of under nondisclosure, obviously, some of the kinds of things that we were doing at Novell.

Q. Mm-hmm.

A. And we were looking at ways -- you know, we viewed Ave -- Aventail as -- as kind of a partner in an ecosystem, so, you know, we would discuss where we were going and, you know, they would discuss somewhat what -- what they were trying to do, as well.

And then we would look at, okay, you know, what kind of extensions were we putting in, and then we'd get into areas like -- one of -- one of the most challenging areas was always the way security is done in SOCKS, and it became that we all centralized on SSL, but, you know, SSL in SOCKS is different. It's -- it's a little bit different than SSL just straight up on TCP, right?

So, in other words, you have to encapsulate SSL in SOCKS, and that was always an area that -- it was kind of bleeding edge in the IETF and, you know --

Page 25

I don't know if you're familiar, but it's always a bit of a challenge from an interoperability standpoint until things are codified, so we -- that would be like an area that we would be working on. There would be, you know, some new cipher or something and some new option. So it always required a little, you know, dinking around with both sides to, you know, get them to talk to each other. Things like that.

Q. Okay.

Were you -- are you familiar with WinSock 2?

A. I'm -- I'm not an expert in WinSock 2, but yes, I know what it is.

Q. What is WinSock 2?

A. WinSock 2 is a -- a -- well, it's a -- it's a plug-in architecture in the WinSock libraries from Microsoft that allow --

Well, first off, it's a Microsoft version of Sockets, modeled loosely after Berkeley, and then WinSock 2 was essentially a Microsoft, I guess, somewhat proprietary standard but modeled after open standards, that had capabilities to put in layered service providers, and that was a -- a way to be able to plug in the underlying network infrastructure that WinSock would run over.

So, in other words, it wasn't -- it wasn't designed just strictly, say, to run only with Microsoft's

Page 26

TCP/IP directly, it was designed to be run over intermediate infrastructure, as well, from a networking standpoint.

Q. Did Aventail provide a product that was a layered service provider?

A. Yes.

MR. LIN: Object to form.

Q. BY MR. KING: Do you recall discussing layered service providers with Aventail during your time at Novell?

A. Minimally. Minimally. I mean, I was familiar with it and I knew that Aventail was using that architecture to build their SOCKS client such that it would not require what is known as socksification. So --

Are you familiar with socksification?

Q. Why don't -- why don't you explain what it is.

A. So in the very beginning, the way SOCKS was designed, it was a requirement of the day -- this would be roughly 1995 to probably -- well, till the layered service provider world came out, that the applications had to actually incorporate the SOCKS mechanisms themselves. So, in other words, there -- there was no provider they could link to like as a library, I mean -- or as an intermediate infrastructure. They had to actually code in SOCKS capabilities. And making an application work with SOCKS was

Page 27

known as socksification.

So I was familiar with Aventail wanting to, you know -- obviously that -- that wasn't a leveraged, you know, type, you know -- an economically leveraged, you know, mechanism to -- to sell your products, right? If you had to go and socksify all of the client applications, that might limit the utility of the SOCKS servers. And so we were familiar that Aventail was -- at Novell was working on layered service providers. They briefed us on that.

And, of course, at Novell we were very interested in this because, you know, if they could make it possible for a wide variety of applications to work over SOCKS without modification, it would probably enable the industry to work -- you know, I mean, it would provide a much larger opportunity for all of us, and we were interested in selling SOCKS servers, so --

MR. LIN: I'm going to object to that -- that question -- that answer as being a narrative and nonresponsive.

Q. BY MR. KING: Do you know whether or not Aventail --

Strike that.

Do you know when Aventail released its first product using what -- that was a layered service provider?

MR. LIN: Object to form.

Page 28

THE WITNESS: Actually, I am not -- I am not sure. I think it was in 1998.

Q. BY MR. KING: Mm-hmm.

Did you know whether or not --

Strike that.

Did Aventail release a -- its layered service provider product before you left Novell in 2000?

MR. LIN: Object to form.

THE WITNESS: Yes, it did.

Q. BY MR. KING: And how do you know that?

MR. LIN: Object to form.

THE WITNESS: Because I used it.

Q. BY MR. KING: What was the name of the product you used?

A. I believe it was called AutoSOCKS.

Q. Now, when did you leave Mi -- when did you leave Novell?

A. July of 2000.

Q. Okay.

Do you remember whether you used this layered -- Aventail's layered service provider product in 1999?

A. Yes. For sure. And I believe probably 1998.

MR. KING: I'm going to mark another exhibit.

(Deposition Exhibit 2 was marked

Page 29

for identification.)
(Discussion off the record.)
Q. BY MR. KING: Do you recognize this document?
A. Yes, I do.
Q. What is it?
A. It's the administrator's guide for the Aventail Connect proxy application.
Q. How do you recognize this document? Where have you seen this document before?
MR. LIN: Object to form.
THE WITNESS: I have seen this document because when we were -- I'm not sure of the correct technical term but served subpoena, I guess to provide information, we went back through our -- our archives and produced information for the years requested, and this was a piece of information that we provided.
Q. BY MR. KING: When you say you went back through your archives, what -- what kind of archives does -- does Aventail maintain?
A. Well, formerly Aventail.
Q. Mm-hmm.
A. Aventail maintained two different repositories of archives. One was source code control that was CVS based in this -- in this time frame, and the other was a -- a document management archive that was LiveLink

Page 30

maintained. This particular piece came from the LiveLink archives.
Q. What is LiveLink?
A. It's a Web-based portal and documentation management system, probably similar to what we would think of as SharePoint today.
Q. Did Exhibit 2 come from your LiveLink database?
A. Yes, it did.
Q. Why was -- why was Exhibit 2 stored in the LiveLink database?
A. It's produced by the -- the technical documentation group.
Q. Mm-hmm.
A. And that group typically does not store things in the source code repository. That's not -- I mean, not the friendliest system for nonprogrammers. So the LiveLink system was used to store all of the sort of non-code-related material in the company, and so the documentation group stored things in there, and they're archived over time by -- by revision and by -- by product.
Q. What does the technical documentation -- what did the technical documentation group at Aventail do?
A. I can only speak since mid-2002.
They would write the administrator's guides,

Page 31

the end user's guides, and also edit some of the technical marketing material and things like that. Not -- not write the copy but do the copy edits. But roughly that -- that type of work.
Q. Were the technical marketing -- were members of the technical marketing group responsible for being familiar with the products they were writing about?
MR. LIN: Object to form.
THE WITNESS: Yes. From what we would think of as a -- a technical white paper point of view, yeah, and in terms of data sheets and things like that, yes.
Q. BY MR. KING: Mm-hmm.
Were these manuals reviewed by developers or others at Aventail who were responsible for creating the products?
MR. LIN: Object to form.
THE WITNESS: I don't know about this one, because it predates me being a part of the organization, but all the documents that were written from mid-2002 on are reviewed by the developers and the management of development, you know, for accuracy.
Q. BY MR. KING: Mm-hmm.
Is it Aventail's general practice to review product manuals for accuracy?
A. Yes.

Page 32

MR. LIN: Object to form.
Q. BY MR. KING: Is it Aventail's general practice to release product manuals that are -- that accurately reflect how its products work?
MR. LIN: Object to form.
THE WITNESS: Yes, as accurately as, you know, we can afford.
Q. BY MR. KING: Are product manuals such as Exhibit 2 given to customers who buy the product?
MR. LIN: Object to form.
THE WITNESS: Yes.
Q. BY MR. KING: Is it part of --
Strike that.
Does Aventail store manuals such as this in its LiveLink database as part of its ordinary course of -- in the ordinary course of business?
MR. LIN: Object to form.
THE WITNESS: It did. SonicWALL now uses --
THE REPORTER: I'm sorry. It's --
THE WITNESS: Yes.
THE REPORTER: It did?
Aventail did during -- yes, until -- until Aventail was acquired.
Q. BY MR. KING: And where -- where are the documents that were stored in the LiveLink database stored

Page 33

now?

MR. LIN: Object to form.

THE WITNESS: They're still in the LiveLink database. It's a -- archive -- I mean, it's a system that's maintained for archival purposes.

Q. BY MR. KING: Okay.

Let's turn to Page i, the first -- the first page.

A. Mm-hmm.

Q. Do you see up at the top it says "© 1996-1999 Aventail Corporation. All rights reserved"?

A. Yes, I see that.

Q. Does that indicate to you when this product manual was released to the public?

MR. LIN: Object to form.

THE WITNESS: No, it does not.

Q. BY MR. KING: Why not?

A. That's a copyright that's spanning material over a several-year duration.

Q. Mm-hmm.

Does that indicate to you that this product was released to the public no later than 1999?

MR. LIN: Object to form.

THE WITNESS: As an individual?

Q. BY MR. KING: Mm-hmm.

Page 34

A. Yeah, I would interpret that.

Q. And why -- why would you interpret that as being -- as showing that it was released in 1999?

MR. LIN: Same objection.

THE WITNESS: I wouldn't say it was re -- well, I would interpret that because I think it is common practice for organizations to update their copyrights to current.

Q. BY MR. KING: Mm-hmm.

A. So -- typically I would find the most advanced year to be the year that it came from.

Q. Is it common practice --

MR. LIN: Object to that answer as being nonresponsive. Excuse me.

MR. KING: Can I hear the question and answer back?

(Record read.)

Q. BY MR. KING: Is it Aventail's ordinary practice to mark its product manuals with a copyright date showing when the -- when the manual was published?

MR. LIN: Object to form.

THE WITNESS: I'm not sure I understand that question exactly.

Q. BY MR. KING: Was it -- was it Aventail's practice to mark its user manuals, such as Exhibit 2, with a

Page 35

copyright date?

A. Yes.

Q. And when Aventail -- would that copyright date be put into the document by a technical writer or someone from the technical writing group?

MR. LIN: Object to form.

THE WITNESS: It would be put in by the documentation group.

Q. BY MR. KING: In your experience at Aventail, does the technical -- is it the technical writing group's standard practice to mark a user manual such as Exhibit 2 with a copyright date showing when the manual was actually finished and published?

MR. LIN: Objection.

THE WITNESS: See, this is where I'm a little bit confused, because you're asking a date, and the copyright is typically a range in time.

Q. BY MR. KING: Okay. So I --

A. It is the practice -- was the practice of Aventail and is the practice of SonicWALL that we maintain our copyrights, so we would be advancing our copyrights each year. If this was produced in 2000 it would say 2000.

Q. And what does it mean that this document says "1996-1999" at the top?

MR. LIN: Object to form.

Page 36

THE WITNESS: My understanding is the material that is contained here within began in some form in 1996 and derivatives of it are spanning through 1999.

Q. BY MR. KING: Okay.

MS. BUCKNER: We've been going for about an hour, Counsel. Do you think we could take a break?

MR. KING: Absolutely.

THE VIDEOGRAPHER: Going off the record. The time is 10:58 a.m.

(Short recess.)

THE VIDEOGRAPHER: We are now back on the record. The time is 11:09 a.m.

Q. BY MR. KING: Referring back to Exhibit 2, I want to ask you a few more follow-up questions. Did Aventail have a technical writing group before you joined in 2002?

A. I -- I don't know that.

Q. Okay. All right.

I'm going to mark as Exhibit 3 a document entitled "Aventail ExtraWeb Server 3.2 Administrator's Guide."

(Deposition Exhibit 3 was marked for identification.)

Q. BY MR. KING: Have you ever seen Exhibit 3 before?

Page 37

A. I have.
Q. What is Exhibit 3?
A. It's the administrator's guide for the ExtraNet Server.
Q. When have you seen this document previously?
A. When we went through the archives looking for information that was being subpoenaed.
Q. That's the LiveLink system?
A. Yes. We found -- I did not. It was found for me by one of my subordinates.
Q. Okay.
Let me just ask a slightly different question. And I apologize for the repetition. Was this document stored in the LiveLink system?
MR. LIN: Object to form.
THE WITNESS: Yes, it was.
Q. BY MR. KING: Who -- who did you ask to search the LiveLink system in order to -- who actually located this document within the LiveLink system?
A. A manager of our documentation department.
Q. Who is that?
A. Mary Siple.
Q. Do you know who wrote Exhibit 3?
A. I do not.
MR. LIN: Object to form.

Page 38

Q. BY MR. KING: Was Exhibit 3 written by Aventail's technical documentation group?
MR. LIN: Object to form.
THE WITNESS: I don't have knowledge of that.
Q. BY MR. KING: Was it Aventail's general practice to have their technical documentation group prepare manuals such as -- such as Exhibit 3?
MR. LIN: Object to form.
THE WITNESS: I don't know if through that time frame.
Q. BY MR. KING: Is it -- was it Aventail's general practice from 2003 through -- through the time of the acquisition to have its technical documentation group prepare product manuals?
A. Yes.
Q. Why did Aventail have its technical documentation group prepare product manuals?
MR. LIN: Object to form.
THE WITNESS: In what time frame?
Q. BY MR. KING: In the -- we'll start with the 2003 time frame, when you were working at -- at Aventail.
A. To provide information to our customers on how to operate our products.
Q. Do you have any -- any reason to believe that was -- that Aventail created product manuals for a different

Page 39

purpose prior to the time that you joined?
MR. LIN: Object to form.
THE WITNESS: I don't have any knowledge of that. Speculating, I would imagine that's what it was for.
Q. BY MR. KING: Mm-hmm.
From 2003 onward was it Aventail's general practice to store product manuals in its LiveLink system?
A. Yes.
Q. And was this product manual stored in -- in the Aventail LiveLink system?
MR. LIN: Object to form.
THE WITNESS: This -- can you rephrase that question?
Q. BY MR. KING: Certainly.
Was Exhibit 3 stored in the Aventail LiveLink system?
A. It -- it is currently stored there.
MR. KING: I'm going to mark as Exhibit 4 a document called "Aventail Connect User's Guide."
(Deposition Exhibit 4 was marked for identification.)
Q. BY MR. KING: Have you seen this document before?
A. Yes, I've seen this document.
Q. What is it?

Page 40

A. This is the end user's guide for Connect proxy.
Q. Where have you seen this document before?
A. I've seen it when we produced it according to a subpoena.
Q. Where was this document stored within Aventail?
A. In the LiveLink archive system.
Q. Mm-hmm.
Is this document a user manual?
MR. LIN: Object to form.
THE WITNESS: This -- yes, this document is intended for end users of Connect proxy to be able to utilize it.
Q. BY MR. KING: Is it Aventail's general practice to prepare user manuals for -- so that its users can correctly operate its software?
MR. LIN: Object to form.
THE WITNESS: In what -- which years?
Q. BY MR. KING: Well, start with the time period that you're familiar with.
A. Yes.
MR. LIN: Object to form.
Q. BY MR. KING: Why was this document stored in the Aventail LiveLink archives?

Page 41

MR. LIN: Object to form.
THE WITNESS: We store all of our user document -- or all of our documentation -- product documentation in the LiveLink archive, until the merger with SonicWALL.
Q. BY MR. KING: So this -- this document states that it's for Version 3.1 of Aventail Connect. Are you familiar with any earlier versions of -- of an Aventail product that are stored in the LiveLink system?
MR. LIN: Object to form.
THE WITNESS: I am not.
Q. BY MR. KING: Do you know how far back in time the archives go in the LiveLink system?
MR. LIN: Object to form.
THE WITNESS: I -- I don't know the -- the -- no, I do not know how far back.
Q. BY MR. KING: Okay.
Let's take a quick break to get this computer up and running.
THE VIDEOGRAPHER: Going off the record. The time is 11:18 a.m.
(Discussion off the record.)
(Deposition Exhibit 5 was marked for identification.)
THE VIDEOGRAPHER: Back on the record. The

Page 42

time is 11:21 a.m.
MR. KING: Thanks.
Q. We've given you on the break what's been marked as Exhibit 5. Can you -- do you mind reading what Exhibit 5 is for the record?
A. It says, "Property of SonicWALL, Inc., Outside Counsel Eyes Only, Source Code, Confidential Information. Aventail ExtraNet Center, 2.6 / 3.1 / 3.2, Source."
Q. Thank you.
In responding to Microsoft's subpoena, did you search for source code that was responsive to the questions that Microsoft asked?
A. Yes.
Q. And where did you search for the source code?
A. In our CVS archive, which is a source code control archive that we maintain for -- not for active use but for archival use.
Q. Mm-hmm.
Can you tell me more?
MR. LIN: Object to form.
THE WITNESS: Tell --
Q. BY MR. KING: Can you describe your CVS archive more fully?
MR. LIN: Same objection.

Page 43

THE WITNESS: Yes. CVS is a -- an open source source code management tool, and it was the management tool that we were using up until 2004.
Q. BY MR. KING: Mm-hmm.
A. All of Aventail's source code prior to 2004 is in there.
Q. When you say "all of Aventail's source code," do you mean all of Aventail's source code starting in 1996?
MR. LIN: Object to form.
THE WITNESS: All that I am aware of.
Q. BY MR. KING: Does that include Version 2 of Aventail's VPN product?
A. It --
MR. LIN: Object to form.
THE WITNESS: It includes that to at least this information. I don't -- I don't know definitively if there's more than that in there.
Q. BY MR. KING: Mm-hmm.
Do you know when Aventail or around what time period Aventail started using the CVS source archive?
MR. LIN: Object to form.
THE WITNESS: I do not know when it was put into place.
Q. BY MR. KING: Okay.
How does C -- how does CVS --

Page 44

Strike that.
What properties does CVS have that allow it to be used as a source code archival system?
MR. LIN: Object to form.
THE WITNESS: CVS maintains a record and version history of -- of all versions of a file, and it's structured in a way that is, you know, common practice for software development.
Q. BY MR. KING: Is CVS used by software developers at the time that they're developing the software?
MR. LIN: Object to form.
THE WITNESS: Yes.
Q. BY MR. KING: Who inputs files into CVS?
MR. LIN: Object to form.
THE WITNESS: A variety of people. Whomever is responsible for a particular file.
Q. BY MR. KING: How do you know when source code is input into CVS?
MR. LIN: Object to form.
Q. BY MR. KING: That was a little unclear. Let me rephrase.
Does CVS track the date and time when source code is input into the system or modified?
A. Yes.
Q. How does it do that?

Page 45

MR. LIN: Object to form.
THE WITNESS: It uses the clock of the server that it's on.
Q. BY MR. KING: Mm-hmm.
And where is this date and time tracking information stored within CVS?
A. It's stored in the attributes, meta-attributes, along with the files.
Q. When you say the attributes, what do you mean?
A. The attributes have information about who did it, what time it was done, and what the chain sets were or the deltas that were applied.
Q. Where are the attributes stored within the CVS system?
A. I -- I don't know the actual structure of CVS.
Q. Mm-hmm.
Does CVS put a time stamp within the actual source code file describing the time when changes were made?
A. Not to my knowledge. It's been awhile since I've looked at CVS.
Q. When you were looking for source code in response to Microsoft's subpoena, what source code did you -- what source code did you extract from the CVS system?

Page 46

A. We extracted all of the source code that was in the time frame that was specified in the subpoena and that was within the scope of what we thought the subpoena was asking.
Q. Mm-hmm.
Do you remember what versions of Aventail's products that included?
A. I do not. I do not remember.
Q. Okay.
Would you mind taking that DVD and putting it into the computer system.
A. (Witness complies.)
Q. Would you please cancel that and open up an Explorer window.
It's probably under My Computer.
A. Ah. Yes.
Q. And open up the DVD.
A. Okay.
Q. What does the top-level directory of the DVD include?
A. It includes different versions of the product.
Q. How do you know that those are different versions of the product that are shown at the top-level directory of Exhibit 5?

Page 47

MR. LIN: Object to form.
THE WITNESS: I know because of the way they're tagged. They're named.
Q. BY MR. KING: Do you recognize these directories?
A. Yes, I do.
Q. How do you recognize -- where have you seen these directories before?
A. These were the directories that my team collected the information and pulled out from CVS.
Q. Once you pulled these directories out of CVS, what did you do with them?
A. Put them on a DVD and gave them to Laurel.
Q. Okay.
Who was it on your team who actually took these directories out of the CVS system?
A. Well, there were several people.
Q. Mm-hmm.
A. Primarily there was Bill Perry and Bryan Sauve.
Q. Did Bill and Perry -- did Bill and Bryan pull this source code out at your direction?
A. Yes.
Q. Would you mind opening up the version --
Let me ask another question. See where it

Page 48

says -- there's a folder titled "V260"?
A. Yes.
Q. What does "V260" mean?
MR. LIN: Object to form.
THE WITNESS: It means Version 2.6.
Q. BY MR. KING: Version 2.6 of what?
A. I have to look in here. I don't recall what's all in here.
Q. Okay. Fair enough.
What does "V310" mean?
A. Version 3.1.
Q. And "V320"?
A. Version 3.6.
MR. LIN: Object --
Q. BY MR. KING: 3.6? Are you sure?
A. Oh. Excuse me. Version 3.2.
Q. Thank you.
Would you mind opening up the Version 3.1 directory.
A. (Witness complies.)
Q. And would you mind reading that. What directory is shown under there?
A. This is SOCKS S5.
Q. What does SOCKS S5 refer to?
A. It refers to Version 5 of the SOCKS server.

Page 49

Q. Mm-hmm.
And would you please open up the SOCKS 5 directory.
A. (Witness complies.)
Q. And what -- what is contained within the Version 5 of the SOCKS directory?
MR. LIN: Object to form.
THE WITNESS: It is the -- I'm not -- I haven't looked at this code for a long time, but from what I can tell, it has both the client and the server for the -- for this version source code contained in it.
Q. BY MR. KING: How can you tell that it contains the code for both the client and the server?
A. There's a directory called AS, and that refers to AutoSOCKS.
Q. Okay.
A. There's a directory called Server, obviously a bunch of server stuff, NT. I'm not familiar with all the structure but, I mean, I can tell that both sides are at least partially contained here, I suspect entirely, given the developers pulled it for me.
Q. How do you know that AS stands for AutoSOCKS?
A. I'm familiar with the source tree. There's nothing that says Connect proxy inside the source tree.
Q. Okay.

Page 50

Is the source tree at the top level similar to source trees that you encountered when you joined Aventail in 2003?
MR. LIN: Object to form.
THE WITNESS: This is different, but it would be similar. It's relative to this particular product set.
Q. BY MR. KING: Okay.
Does the V -- does the Version 3.1 directory on Exhibit 5 correspond to Aventail Connect Version 3.1 -- the Aventail Connect Version 3.1 manuals --
Let me start over.
Would you pull out Exhibit 2 for a second.
A. Yes.
Q. Mm-hmm.
A. Mm-hmm.
Q. Exhibit 2 states that it's for Version 3.1 and 2.6 of Aventail Connect, right?
A. It does.
Q. Does the Version 3.1 on Exhibit 2 correspond to Version 3.1 in the source code DVD that we've marked as Exhibit 5?
MR. LIN: Object to form.
THE WITNESS: I'm told by a person who is familiar with it that it does.
Q. BY MR. KING: Who -- who told you that?

Page 51

MR. LIN: Object to form.
THE WITNESS: Bryan Sauve.
Q. BY MR. KING: How does Bryan know that they -- that Version 3.1 --
A. He --
MR. LIN: Object to form.
Hold on.
Object to form.
Q. BY MR. KING: Let me back up. How does Bryan know that -- that this manual corresponds to the source code on -- labeled Version 3.1 on Exhibit 5?
MR. LIN: Object to form.
THE WITNESS: Bryan was a developer who worked on Version 3.1.
Q. BY MR. KING: Mm-hmm.
Let's go to Version 2.6 on the source code DVD, Exhibit 5.
And I'll note for the record that you just entered the SOCKS S5 directory.
A. Oh, excuse me. Excuse me. I'm sorry. I went a little fast.
Yes. SOCKS S5 is the first.
Q. Would you mind opening up the SOCKS S5 directory.
A. Yes, I will do that.

Page 52

Q. What is shown within the SOCKS S5 directory of the Version 2.6 branch of the source code?
A. I believe it shows the entire set of source for the 2.6 product. Both the client and the server.
Q. Where is the server code stored within Version 2.6 of the source code branch?
MR. LIN: Object to form.
THE WITNESS: Well, it's primarily in server, but, again, source code does have referrals across common code.
Q. BY MR. KING: And where is the client code for Version 2.6 stored within this directory?
MR. LIN: Object to form.
THE WITNESS: It's primarily stored in the AS directory.
Q. BY MR. KING: AS stands for AutoSOCKS?
A. AutoSOCKS.
Q. Okay.
Do you know whether the Version 2.6 of the source code on the source code DVD corresponds to Version 2.6 of Aventail Connect as described in Exhibit 2?
MR. LIN: Object to form.
THE WITNESS: I -- I don't know firsthand that. I believe it does.
Q. BY MR. KING: Why do you believe that it

Page 53

does?
A. Because --
MR. LIN: Object to form.
THE WITNESS: -- the developer told me it did.
Q. BY MR. KING: And this is Bryan --
A. Yes.
Q. What was his last name?
A. Sauve.
Q. Sauve. Okay.
Let's go to the Version 3.2 branch on Exhibit 5.
A. Yes.
Q. Can you open that up?
A. Yes.
Q. What's shown within the Version 3.2 branch?
A. SOCKS S5.
Q. Would you mind opening the SOCKS S5 directory.
A. Yes.
Q. Can you describe what is contained within the SOCKS S5 directory?
A. I believe it has the entire source for the 3.2 product, both the client and server.
Q. And where is the server code primarily stored

Page 54

within this directory?
MR. LIN: Object to form.
THE WITNESS: It's primarily stored in the server folder.
Q. BY MR. KING: Where is the client code primarily stored within this directory?
A. In the --
MR. LIN: Same objection.
THE WITNESS: -- AS folder.
MR. LIN: Did you get my objection?
THE REPORTER: Yes.
Q. BY MR. KING: Does the Version 3.2 folder on Exhibit 5 correspond to Exhibit 3, the Aventail ExtraNet Center Version 3.2 administrator's guide?
MR. LIN: Object to form.
THE WITNESS: Yes, I believe the server does.
Q. BY MR. KING: Mm-hmm.
And why do you believe that the source code corresponds to Exhibit 3?
MR. LIN: Object to form.
THE WITNESS: Because a developer vouched for it.
Q. BY MR. KING: And which developer was that?
A. Bill Perry.
Q. Okay.

Page 55

How does Bill Perry know that the Version 3.2 of the source code as contained in Exhibit 5 corresponds to the Aventail ExtraNet Center Version 3.2 manual that we've -- that we're talking about with Exhibit 3?
MR. LIN: Object to form.
THE WITNESS: Bill Perry developed part of the ExtraNet Server.
Q. BY MR. KING: Who at Aventail -- or who at SonicWALL is responsible for maintaining the CVS tree at the present time?
A. It's not actively used anymore.
Q. Mm-hmm.
A. Our build master is responsible for maintaining the archive.
Q. And who is your build master?
A. Wade Valentine.
Q. Who does -- does Wade Valentine report to you?
A. Not anymore.
Q. Did he report to you in the past?
A. Yes.
Q. What was your -- what was your title when he reported to you?
A. Chief architect and director of software engineering.

Page 56

Q. Okay.
Was Wade Valentine, at the time he reported to you, your build master?
A. Yes.
Q. Was he responsible for maintaining the CVS tree?
A. Maintaining the system, yes, as an archive.
Q. Okay.
Is it Aventail's ordinary course of business to --
Or strike that.
Was it Aventail's typical business practice to store source code in -- in the CVS system?
MR. LIN: Object to form.
THE WITNESS: Yes, at that time.
Q. BY MR. KING: Mm-hmm.
And was developing source code one of Aventail's standard business activities?
MR. LIN: Object to form.
THE WITNESS: It has been since I have been an employee, yes.
Q. BY MR. KING: Okay.
Going to mark two more exhibits.
(Deposition Exhibits 6 and 7 were marked for identification.)

Page 57

THE WITNESS: Yes.
Q. BY MR. KING: Mm-hmm.
So you're -- we've handed you Exhibits 6 and 7, which are two files of source code that I'll represent to you came from Exhibit 5.
Have you ever seen -- let's start with Exhibit 6. Have you ever seen a document -- have you ever seen Exhibit 6 before?
MR. LIN: Object to form.
THE WITNESS: I might have seen it before. I don't recall whether I've actually looked at the source or not.
Q. BY MR. KING: Mm-hmm.
Have you ever seen doc -- are you familiar with documents like this at Aventail?
MR. LIN: Object to form.
THE WITNESS: Yes.
Q. BY MR. KING: What -- what is Exhibit 6?
A. This is source code. Source code to the AutoSOCKS redirector.
Q. What is the AutoSOCKS redirector?
A. That's part of the layered service provider that takes requests that are coming in from applications and redirects them into the VPN.
Q. Mm-hmm.

Page 58

A. It's part of that system.
Q. Okay.
Do you see the first half of this page has a slash and then a line of -- of asterisks going down the side?
A. Yes.
Q. What does -- what does the slash and that line of asterisks indicate?
A. It means that these are comments.
Q. Mm-hmm.
And what do these -- we'll start with the first comment up at the top, where it says "$Header."
A. Yes.
Q. What does that comment indicate to you?
A. That would have been produced by CVS.
Q. Mm-hmm.
When you say it was produced by CVS, what do you mean?
A. CVS put its time stamp in there when it was -- and I'm not sure. I think when it was checked in.
My knowledge of CVS is starting to get old.
Q. Okay.
So where is the time stamp within the -- the first header of Exhibit 6?
A. It's at the top of the comments.

Page 59

Q. Mm-hmm.
And when does it say that Exhibit 6 was marked by CVS?
A. February -- let's see. Ooh. Let me think.
You know, I'm -- I'm not sure. I'd have to look it up. It's either February 8th or August 2nd. I don't remember the order that CVS puts these out. At 1:22 in the afternoon.
Q. That's the 1322?
A. 1322.
Q. Okay.
Do you see at the right-hand side of the first line where it says "v 1.5"?
A. Yes.
Q. What does that mean?
A. That's the specific version of this source file.
Q. Did CVS always put time -- time and date stamps like this at the top of files when they were checked in?
MR. LIN: Object to form.
THE WITNESS: I would have to actually examine the source code to answer that. I don't know.
Q. BY MR. KING: Mm-hmm.
A. I think it does.

Page 60

Q. Have you seen -- you've seen headers like this before?
A. I have.
Q. Okay.
A. Yes.
Q. Let's turn to the -- the end of -- of Exhibit 6.
A. Which -- which page? The very end?
Q. I guess it's three pages from the end, where the comments begin.
A. Yes.
Q. Do you see where it says "$Log"?
A. I do.
Q. What does that refer to?
A. This is CVS information that it's maintaining for revision history.
Q. And what -- what is revision history?
A. Talks about various check-ins that have been done to the code.
Q. Mm-hmm.
Do you see where it says "Revision 1.5 1999/02/08"?
A. I do.
Q. What does that refer to?
A. I think I can actually refer -- now I can see

Page 61

it because I can see the next one down.
That would be February 8th, 1999. A fifth revision was done to this. I think this would be a more major branch.
My CVS is getting old now.
And it was done by the initials DB.
Q. What do those initials refer to?
A. Derek Brown.
Q. Who is Derek Brown?
A. He's one of the founders of Aventail who wrote the original AutoSOCKS.
Q. Is Derek Brown a software developer?
A. Yes.
Q. Let's go -- do you see below that it says, "Remerge the stuff from the branch back to the trunk"?
A. Yes. So --
Q. Why -- why is that statement contained within Exhibit 6, if you know?
MR. LIN: Object to form.
THE WITNESS: My interpretation --
Q. BY MR. KING: Mm-hmm.
A. -- as -- as a software developer?
This is a comment stating that other branches had changes made that needed to be merged back into the main trunk. So probably one of the earlier versions of the

Page 62

product had changes made that were being merged back into the currently under development version.
Q. What is a trunk within CVS terminology?
A. CVS is -- you can have branches, so like a product branch typically would be branched, some instance, and the trunk is kind of where all the sort of continuum is going on. So you take snapshots in time that are called branches, and you can make modifications there that are unique to that particular branch. And if you need to have them in any other branch, you have to merge them.
The trunk is kind of the continuum over time, right? Does that make sense?
You take a branch of code in time. Trunk just continues on.
Q. Okay.
Let's go back to the first page of Exhibit 6. Do you see at the top of the first CVS header where it says, "/usr/aventail/prodroot," et cetera?
A. Yes.
Q. And then it says "sockss5" after that?
A. Yes.
Q. Does that "socksf5" -- what does that "socksf5" refer to?
MR. LIN: Object to form.
MR. KING: Sorry. "Sockss5," just for the

Page 63

record.
THE WITNESS: So the -- the actual CVS repository was on a Unix system and not a Windows system. This is a Unix path.
I can't state definitively because I can't see this, but it's probably referring to the same SOCKS 5 that we're seeing here under the -- each of these versions. I don't know which particular version this -- this came from.
Q. BY MR. KING: Would you see if you can find this file within the Version 3.1 branch of Exhibit 5?
A. Yeah. Let's see. Probably going to be under AS.
Q. I think you're under the Version 3.2 branch right now.
A. Am I under -- you are correct.
Okay. So I've gone into AS, and then I go into WIN. I'm going to go into S5HOOK.
Do you see an S5HOOK up here?
Yeah. Okay.
And REDIR.CPP is probably -- yup. Probably right here.
Ooh. This is Unix.
Q. Maybe you can open it with WordPad instead of NotePad.

Page 64

A. That's probably a good idea.
Okay.
Yeah, it looks remarkably similar, huh? 1322. February 8th.
Q. Does the file you're looking at on Exhibit 5 have the same CVS header?
A. Yes, it has the same CVS header.
Q. All right.
And can you use that CVS header to determine --
Strike that.
Let me ask you another question.
Let's go to Exhibit 7.
A. Yes.
Q. What is Exhibit 7?
A. Appears to be the same as Exhibit 6, but I'm not sure.
I don't know where this actually originated from.
Q. Well, I'll represent to you --
Let me start over. Do you see the top CVS header?
A. Yes.
Q. Does that provide you with any indication of what this -- of what Exhibit 7 is?

Page 65

MR. LIN: Object to form.
THE WITNESS: It does, although it looks to be the same to me as Exhibit 6.
Q. BY MR. KING: Can I see that?
A. Mm-hmm.
Q. You are correct.
Let me see if I can fix that.
All right. I guess we had a copy error.
A. Okay.
Q. Let's go back to Exhibit 6.
A. Yes.
Q. Looking again at the CVS time stamp, what -- how did CVS generate that -- the time stamp shown at the top of Exhibit 6?
MR. LIN: Object to form.
THE WITNESS: From what I know of CVS, it used the then current time that this was checked in by Derek Brown to generate that -- that additional header. If you notice, that's actually a -- a separate comment.
Q. BY MR. KING: Mm-hmm.
And when you say "the then current time," what -- what do you mean?
A. When Derek committed this change, there is a command that when you're done coding and doing whatever you're going to do you commit it, and it -- it was at that

Page 66

time the system actually took a time stamp as it was committing it into the archive.
Q. Okay.
Let's go back to Exhibit 5. If you could close down the WordPad --
Sorry. We're going back to Exhibit 5 on the computer.
A. Okay.
Q. If you could close down the WordPad file.
A. Yes.
Q. Can you change the Internet Explorer window so that it shows times and dates on -- or the time and date those files were modified?
A. Yeah, this is --
This right here?
Q. That's correct.
A. Yes.
Q. Okay.
Now, can you find the time and date that REDIR.CPP was -- was modified?
MR. LIN: Object to form.
THE WITNESS: Oh. This says February 7th, 1999, at 4:13.
Q. BY MR. KING: What does that -- what is the significance that -- of --

Page 67

Are you familiar with the way in which files obtain date modified notations within -- within operating systems?
MR. LIN: Object to form.
THE WITNESS: Yeah, at one time I was pretty familiar with the Unix.
Q. BY MR. KING: Mm-hmm.
What does it mean when it says date mod -- a date modified of February --
A. I believe this means this was the last time that there was a write operation performed on it.
MR. LIN: I'm going to object -- object to that question.
Q. BY MR. KING: Is it unusual that that date on REDIR.CPP is different from the CVS header that we saw on a printed -- on the printed version of REDIR.CPP as Exhibit 6?
MR. LIN: Object to form.
THE WITNESS: I can't account for that. I don't know why that is.
Q. BY MR. KING: Okay. All right.
Let's go to -- go back to Exhibit 2.
Exhibit -- can you tell me what -- what Aventail Connect is?
MR. LIN: Object to form.
THE WITNESS: Yes. Aventail Connect is a --

Page 68

a marketing name for a product that is a -- or was a -- a VPN client that would redirect application traffic into a -- a SOCKS-based VPN server.
Q. BY MR. KING: How would -- you said Aventail Connect is a VPN client, right?
A. Yes.
Q. What does that mean that it's a VPN client?
MR. LIN: Object to form.
THE WITNESS: By Aventail definition, it means that it is a piece of software that will securely connect an application on the client side with a service or an application on the server side that's located through a cryptographically protected tunnel, so that you can use information on servers that are on other networks securely from typically an insecure network that you're on at that point. The end user.
Q. BY MR. KING: The end user.
Is Aven -- where is Aventail Connect installed?
MR. LIN: Object to form.
THE WITNESS: It's installed on Windows-based clients.
Q. BY MR. KING: Is it -- how do end users use Aventail Connect?
MR. LIN: Object to form.

Page 69

THE WITNESS: They use it to establish a secure communications channel to remote resources that they want to keep confidential.
Q. BY MR. KING: Mm-hmm.
Is Aventail Connect installed on an end user's computer?
A. One who's going to use this particular VPN, yes.
Q. Okay.
Can we go to -- let's go to Page 7 of the administrator's guide, Exhibit 2.
Do you see the second paragraph from the bottom, last sentence, "Aventail Connect does not require administrators to manually establish an encrypted tunnel; Aventail Connect can establish an encrypted tunnel automatically"?
A. Yes.
Q. Can you tell me what that means?
MR. LIN: Object to form.
THE WITNESS: Yeah. I can tell you what it means. The -- the interpretation in this -- in this instance is the -- the application does not have to initiate any kind of cryptography on its own. They connect -- a proxy client will automatically initiate that cryptography when the connection is placed through the VPN.

Page 70

Q. BY MR. KING: Does the user have to do anything to initiate the cryptography?
MR. LIN: Object to form.
THE WITNESS: They have to do one thing. They have to log into the VPN prior, and then while they're logged in, all applications going to resources in the VPN will have the cryptography automatically instantiated for them.
Q. BY MR. KING: How did -- what do users have to enter into the computer in order to log into the VPN?
MR. LIN: Object to form.
THE WITNESS: They have to connect to the server, and they have to pass some authentication challenges.
Q. BY MR. KING: What sort of authentication challenges do they have to pass?
MR. LIN: Object to form.
THE WITNESS: That depends on the kind of authentication that the administrator has chosen.
Q. BY MR. KING: Mm-hmm.
A. There are different forms. One would be user name and password, very typical. Another form might be -- in the Connect supported is challenge response, so multifactor tokens, where you know more than just a user name, a user name and a PIN and some random number

Page 71

generator, things like that. But that's -- that's based on what the administrator chose for the authentication.
Q. Does the user have to enter any cryptographic information when logging into the VPN under the user name and password scenario?
MR. LIN: Object to form.
THE WITNESS: No, not -- not as I would consider cryptographic. I mean, nothing outside the scope of what I just said.
Q. BY MR. KING: Mm-hmm.
What about in the multiform scenario, in that scenario does the user have to enter any cryptographic information?
MR. LIN: Object to form.
THE WITNESS: No.
Q. BY MR. KING: Let's go to Page 11.
Do you see where it says "How Does Aventail Connect Work?"
A. Yes.
Q. I want to spend a couple minutes and just walk through Page 11 and Page 12 and Page 13 and have you describe for us how Aventail Connect works. Is that fair?
A. Yeah. I might have to read this a little bit with you.
Q. That's fine.

Page 72

A. I haven't seen this for a while.
Q. That's fine.
Let's -- actually -- let's start with Page 10.
Not even Page 10. Page 9. Where it says "What Does Aventail Connect Do?"
A. Yes.
Q. Do you see that -- that picture on Page 9?
A. Yes, I see, yes, protocol stack.
MR. LIN: Tom, can I lodge a standing objection at this point to form as to all the questions regarding AVN 00015 and 00016?
MR. KING: What's the basis for your objection?
MR. LIN: The witness has -- did not prepare this document. He wasn't employed by Aventail at the time this product was released. Lacks foundation, personal knowledge.
MR. KING: Okay.
MR. LIN: Yeah.
MR. BRIGHT: Tom, just to be clear, is that okay that we have a standing objection, or do you want us to lodge the objection to every question?
MR. KING: I'm not sure that's an objection to form, so I don't -- I don't -- you can do --

Page 73

MR. BRIGHT: What we feel necessary?
MR. KING: -- what you feel necessary.
MR. BRIGHT: Okay.
MR. KING: And I'll note that if it's not an objection to form, you'd be waiving it by stating it on the record.
MR. BRIGHT: You can note what you want.
Q. BY MR. KING: What does the figure on Page 9 of Exhibit 2 show?
MR. LIN: Object to form.
THE WITNESS: It is a representation of how Microsoft networking stacks were composed in Win 95.
Q. BY MR. KING: And can you walk me through this figure and explain to me what it shows?
A. Yeah, to the best of my ability, I can.
Q. Mm-hmm.
A. The top box refers to an application that's running on Windows 95 that -- that is going to use the TCP/IP protocol, and it's going to consume that -- or it's going to interface with TCP/IP either through the older WinSock 1.1 API or the newer WinSock 2 API.
MR. LIN: I'm going to object to the previous question.
THE WITNESS: The box immediately below it, that says WinSock 2, is describing the WinSock 2 sort of

Page 74

block architecture, in that the application can directly use WinSock 2 through the right arrow. That's a -- that was the more modern API of the day. And on the left, the WinSock 1.1 interface was also for compatibility provided by the WinSock 2 provider. So it could -- either a WinSock 1.1 or a WinSock 2 client or application could use the WinSock 2 API.
And then in the middle, it says "Aventail Connect (Layered Service Provider)," and over on the right it says, "Multiple LSPs can be installed at this level." So the -- what that is saying is the Aventail Connect is actually implemented as a layered service provider in the Win -- WinSock 2 architecture and that the -- and it may coexist with other WinSock providers.
And when an application makes a call to WinSock 2, it ultimately will pass through the Aventail Connect provider, who will inspect it and decide what to do, and once the Aventail Connect has decided what to do, the traffic will be passed on to the TCP/IP stack, where it will be forwarded on whatever the physical connector is, such as, say, ethernet.
Q. BY MR. KING: Were you familiar with this architecture -- architectural model during the time that you were at Novell?
MR. LIN: Object to form.

Page 75

THE WITNESS: Yes.
Q. BY MR. KING: What was your -- was your understanding of how Aventail's products work -- worked in 1999 consistent with this model as shown in Aventail Connect -- in the Aventail Connect 3.1 manual that is Exhibit 2?
MR. LIN: Object to form.
THE WITNESS: Yes.
Q. BY MR. KING: Let's go to Page 11.
And you'll see that Page 11 through 13 has a number of numbers and bullet points, Step 1, 2, 3, and then some bullet points. Do you see that?
A. I do see that.
Q. Let's start with -- would you take a minute to -- to read Pages 11 through 13.
A. Yes, I will.
Okay.
Q. Okay.
We need to change the tape, so why don't we just take a quick break.
THE VIDEOGRAPHER: Going off the record. The time is 12:11 p.m.
(Discussion off the record.)
(Short recess.)
THE VIDEOGRAPHER: This marks the beginning

Page 76

of Tape No. 2. Back on the record. The time is 12:17 p.m.
Q. BY MR. KING: Referring to Exhibit 2, do you see Paragraph No. 1 on Page 11?
A. Yes.
Q. Would you mind reading that into the record?
A. Starting with --
Q. Starting with, "The application."
A. On which page?
Q. On Page -- sorry. Page 11.
A. 11? Yeah.
Q. See where it says, "1. The application does a DNS lookup"?
A. Oh, oh, oh. Okay. Excuse me. Okay. Yes. Okay. All right.
"The application does a DNS lookup to convert the hostname to an IP address or, in rare cases, it will do a reverse DNS lookup to convert the IP address to a host name. If the application already knows the IP address, the entire step is skipped. Otherwise, Aventail Connect does the following."
Q. What does -- can you explain -- explain to me what Paragraph 1 means?
MR. LIN: Object to form.
THE WITNESS: Yes. So most of the time an application is actually looking up something by name --

Page 77

Q. BY MR. KING: Mm-hmm.
A. -- such as, say, www.google.com, and so there's a system called DNS, or the Domain Name Service, which will try and convert a name into an IP address. Applications can't connect directly to names, they have to connect to addresses. So what it's saying is it -- most likely the application is going to do a DNS name, and sometimes it's the opposite. Sometimes it knows an IP address name but it wants to know a name for it. That's not a typical kind of thing, but if that's the case, the DNS system can be programmed to reverse it.
Q. Let's put reverse DNS to the side for now.
A. Reverse. Yeah, it's not probably --
That's what that means.
Q. Mm-hmm.
What sort of applications could use Aventail Connect 3.1?
MR. LIN: Object to form.
THE WITNESS: Well, from what I recall of 3.1, any TCP/IP application that's initiating a connection out.
Q. BY MR. KING: Can you give me some examples of programs that use TCP/IP?
A. Mm-hmm.
MR. LIN: Object to form.

Page 78

THE WITNESS: Outlook, the mail reader, FTP would do it. Web, so use IE would do it.
Q. BY MR. KING: IE is what?
A. Internet Explorer.
Q. Where does your familiarity of Aventail Connect 3.1 come from?
MR. LIN: Object to form.
THE WITNESS: It comes as -- as a user of it, not -- not -- not a heavy user of it but a user of it in testing with Novell products.
Q. BY MR. KING: That was during the -- the 1999 time frame?
A. Yeah. Ninety -- yeah, between 1998 and 2000, so --
Q. BY MR. KING: Okay.
Let's go to the next paragraph. Do you see where it says, "If the hostname"?
A. Yes.
MR. LIN: Object to form.
Q. BY MR. KING: I won't ask you to read that for the record, but would you mind explaining to -- you know, with that paragraph in mind, would you mind explaining to me what Aventail Connect did when it received a DNS lookup request from an application?
MR. LIN: Object to form.

Page 79

THE WITNESS: Yeah. So the Aventail Connect component had a set of rules that defined the servers and application, primarily it would be servers, servers that were in the VPN, that the traffic should be intercepted and redirected through the VPN, the cryptographically protected VPN. And so the Aventail Connect ran inside the LSP, meaning that all of the communications coming down it could intercept and look at. So it wanted to see if a DNS name that was coming down was in the redirection set.
Q. BY MR. KING: When you say it was wanted -- it wanted to see whether a DNS name was in the redirection set, can you explain to me what that means, and maybe --
A. Yeah. So --
Q. In the way that you would explain to it a layperson?
MR. LIN: Object to form.
THE WITNESS: Yeah. So I'll give you two examples of how this would sort of -- when it would intervene and when it would not. So let's say that it sees a name www.myco.com, and that name is a name that the administrator of the VPN has registered as being inside the VPN. Okay. So when a request comes in, let's say it's in Internet Explorer, so you type www.myco.com, and the Aventail Connect proxy sees this, because it's sitting in the -- it's filtering all the traffic coming from the

Page 80

application from WinSock. It says, Oh, that matches a rule that's in the VPN. I'm going to have to intercept that and begin doing some of these other operations that -- that are described here. Okay?
As opposed to, let's say that you were saying www.google.com, right? A public name, not programmed for redirection by the VPN administrator. Aventail Connect would look at that and say, Oh. That's not in the redirection set. Do not, you know, intercept this request, just let it flow on through, without any disturbance by the Aventail Connect. That's so that it could go out through a different provider.
Q. BY MR. KING: How did the Aventail Connect proxy determine whether the DNS request should be sent to the DNS server as opposed to --
Or sorry. Let me strike that.
How did the Aventail Connect proxy determine whether to direct traffic to a VPN or not?
MR. LIN: Object to form.
THE WITNESS: It used a configuration file that was stored on the client that contained all the redirection rules, so when it loaded it read that in, and then it used that as a rule set to look at against connection -- or name requests coming through.
Q. BY MR. KING: Did redirection rules specify

Page 81

whether or not a host name corresponded to a secure target?

MR. LIN: Object to form.

THE WITNESS: Well, you know, I don't have firsthand knowledge from this era.

Q. BY MR. KING: Mm-hmm.

A. From the year 2002 on, there's no -- there's no information in there as to whether that -- that was a -- a secure site or not.

Q. How did Aventail Connect determine whether or not to send traffic over a VPN, then?

MR. LIN: Object to form.

THE WITNESS: Yeah. Let me read the rest of these steps.

Q. BY MR. KING: Mm-hmm.

A. What it would do is it would need to determine if the request coming in was either a name that is in the VPN or an address that's in the VPN. The rules could be either. If -- if it is a name, it has to get a name translated to an address, because the -- the actual connect request is going to come from an application, it's not going to be a name. You can't say connect to and then a name, right? You have to connect to an address.

So in the case that it's a name, it has to convert it to an address that it can subsequently intercept, right? So it's going to say, Oh. Here's a name. It needs

Page 82

to be resolved within the -- the VPN. And it would do that by essentially impersonating the -- the DNS system, and it would -- it would forward the -- the request to the server, and the server would attempt to resolve it by name inside the remote network. And then if the name was resolved, the server responds to the client and tells him what the actual real address is. And then the client, Aventail Connect, would generate a fake IP address and give it back that it would remember, so it would tag it and give kind of a fake address that -- that would go back to the -- to the client application.

And then when the client application subsequently makes the connect request, it wants to establish a TCP connection, it would intercept either the fake address or an address that's in the redirected namespace, that's a rule, and basically divert that into its SSL -- or a SOCKS tunnel.

And that's essentially what this whole thing is saying here.

If it's not an address that's in the redirection set, it would not redirect it, it would just pass it on through to whoever the next provider is.

Q. Was a -- was a user -- was an end user aware that any of this was happening behind the scenes when they used Aventail Connect?

Page 83

MR. LIN: Object to form.

THE WITNESS: Not typically. A user could be, if they wanted to understand how to program the client, but typically that would be done by the administrator, and the user didn't really know unless they were challenged by the VPN to -- to log in.

Q. BY MR. KING: Did -- did Aventail Connect allow applications to connect directly to the target computer through a VPN, or did all communications have to go through the SOCKS server?

MR. LIN: Object to form.

THE WITNESS: They would have to go through the SOCKS server.

Q. BY MR. KING: Why -- why did all communications have to go through the SOCKS server?

MR. LIN: Object to form.

THE WITNESS: They had to be put into a cryp -- well, typically cryptographically protected. It's possible to run SOCKS without it, but typically an SSL-encrypted tunnel in SOCKS, so what it had to do is it had to take the requests from the client and redirect them into a tunnel that was cryptographically protected, and that tunnel was a connection between the physical client and the SOCKS server, and traffic would transit on this encrypted connection, at which point the server would take it out of

Page 84

the tunnel and then forward it on to the correct IP address using just routed -- you know, routing inside the VPN.

Q. BY MR. KING: Mm-hmm.

Did the server have a -- have a VPN connection to the target computer?

MR. LIN: Object to form.

THE WITNESS: No.

Q. BY MR. KING: Was the Aventail Connect client aware of the real IP address of the target computer?

MR. LIN: Object to form.

THE WITNESS: I -- I don't recall.

Q. BY MR. KING: Mm-hmm.

Do you see at the bottom of Page 12, the last partial sentence, "From the applications point of view, the entire SOCKS negotiation, including the authentication negotiation, is merely the TCP handshaking"?

It's the last sentence of Page 12, and then going on to Page 13.

A. Yes, I see that.

Q. Can you tell me what that sentence means?

MR. LIN: Object to form.

THE WITNESS: Yes. The -- yes. So the -- the TCP connection itself can't be completed until the SOCKS negotiation is done and the tunnel. In SOCKS these -- these were not multiplex, so the -- each and every individual

Page 85

connection being made by a client application had a separate TCP/IP connection to the server that was going -- that was SOCKS encapsulated, and so the process of establishing the SOCKS communication was done transparently to the application, such that its request was held up while the Connect proxy actually contacted the server, negotiated it all out, and once -- if it got, you know, a clean tunnel up, then it would allow the TCP/IP traffic to flow through and complete the TCP handshake.

Q. You said it was transparent to the application. Does that also mean that it was transparent to the end user?

MR. LIN: Object to form.

THE WITNESS: Yes.

Q. BY MR. KING: I'll just wrap up with a few questions going back to your time at Novell. You said that Novell -- was Novell interested in developing a WinSock 2 layered service provider VPN?

A. No.

Q. No?

Why not?

MR. LIN: Object to form.

Q. BY MR. KING: Actually, strike that. Let me ask a different question.

Are you aware of anybody other than Aventail

Page 86

who developed a WinSock 2 layered service provider VPN?

A. No.

MR. LIN: Object to form.

Q. BY MR. KING: Aventail is the only one you're aware of?

A. In that era.

Q. Okay.

All right. Well, that's all of the questions I have for now. Why don't we break for lunch.

THE VIDEOGRAPHER: Going off the record. The time is 12:33 p.m.

(A luncheon recess was taken at 12:33 p.m.)

---o---

Page 87

SEATTLE, WASHINGTON; FRIDAY, FEBRUARY 27, 2009

1:35 P.M.

--o0o--

THE VIDEOGRAPHER: Back on the record. The time is currently 1:35 p.m.

E X A M I N A T I O N

BY MR. LIN:

Q. Now the roles are reversed. I'm going to be asking you some questions.

Do you understand that you're still under oath?

A. I do.

Q. Okay.

If I could have you turn to what's previously been marked as Exhibit 2.

A. Yes.

Q. Is it correct, sir, that you did not prepare Exhibit 2?

A. I did not prepare it, no.

Q. Have you ever seen this document before, Exhibit 2?

A. I have seen it, yes.

Q. When did you see this document?

Page 88

A. I saw it when we were asked to produce information.

Q. Have you ever seen Exhibit 2 prior to being asked to produce information?

A. I think I did, but I'm -- I'm not exactly sure.

Q. So you don't -- so you don't know that you reviewed this precise version of Exhibit 2?

A. I don't know that I ever reviewed this one.

Q. Okay.

And do you know who maintained custody of Exhibit 2 from the time it was first produced until the time that you joined Aventail?

A. I don't know for sure when it was first produced. I know who had custody when I did join Aventail, and that was Scott Boggan.

Q. Do you have any personal knowledge as to who maintained custody of this document prior to you joining Aventail?

A. I do not.

Q. And do you have any personal knowledge as to when this document was published?

A. I do not.

Q. And have you ever reviewed this document to confirm the accuracy of the contents of Exhibit 2?

Page 89

A. Yes, I have reviewed it with our developers with respect to the source code.
Q. And when was that?
A. December of 2007.
Q. And was that in response to receiving the subpoena by Microsoft?
A. Yes.
Q. Who did you speak with to verify the accuracy of the contents of Exhibit 2?
A. Bryan Sauve.
Q. And who is Bryan Sauve?
A. He's a former Aventail and SonicWALL employee who was a developer of Connect.
Q. When did Bryan Sauve depart from Aventail?
A. He departed from SonicWALL in September of 2008.
Q. And can you describe the steps that you took to confirm the accuracy of the contents of Exhibit 2 with respect to the source code?
A. Yes. We matched the source code up against the descriptions in this document.
Q. And how much time did you spend verifying the contents of Exhibit 2?
A. Less than one day.
Q. And how many source code files are --

Page 90

Excuse me. How many source code files are there for the versions of Aventail Connect described in Exhibit 2?
A. That I don't know off the top of my head.
Q. Would it be more than a thousand files?
A. No, I don't believe it's more than a thousand files.
Q. Can I direct your attention to Exhibit 5, and if you --
A. Yes.
Q. -- will reman the computer.
Could you -- could you go to the root directory, the C, please.
A. (Witness complies.)
Q. Is that the root directory?
Thanks.
A. Okay.
Q. Could you please open the file that -- excuse me -- open the folder that corresponds to Version 3.1?
A. (Witness complies.)
Q. And can you do a right click on that SOCKS 5 folder?
A. Yes.
Q. And click on Properties?
A. Yes.

Page 91

Q. And how many files are in that folder?
A. There's 4,000 files, of which the lion's share I believe are on the server side.
Q. Okay.
So it's your testimony that on the Connect side --
A. Yeah, I -- I don't know exactly how many. I'd have to sit down with the guys.
Q. Okay.
A. The server is considerably larger than the -- than the client.
Q. And did you review every single source code file for Aventail Connect Version 3.1?
A. No, we did not go through every single file.
Q. How many files, approximately, did you go through with Mike Sauve?
Did I get the name correct?
A. Oh, Bryan.
Q. Bryan.
A. Bryan Sauve. It's S-a-u-v-e.
I don't recall how many.
Q. And did you do a page-by-page analysis in Exhibit 2?
A. Not in depth.
Q. Not in depth?

Page 92

A. Not in depth.
Q. And when you identified a feature described in Exhibit 2, did Bryan Sauve direct you to the relevant source code?
A. He did not go source file by source file, as he was aware of what -- what the entire tree was.
Q. So to what extent did you review the contents of Exhibit 2 in connection with the source code?
A. We verified that the source that we had pulled in Exhibit -- oh -- that what is described in Exhibit 2 was matched up with what we had found in the source.
Q. And how did you determine what was pulled from the source matched what was described in Exhibit 2?
A. If I recall, we looked at the configuration file, primarily, to see if it lined up correctly with what was described in here, and then we matched the time of the archives between the LiveLink as well as the CVS, to confirm they were from the same epoch.
Q. So you confirmed that the source code was approximately developed at the same time as Exhibit 2? Is that what you're saying?
A. That was our intent.
Q. And which of the source code files in Exhibit 5 did Bryan Sauve write?

Page 93

A. That I'm not sure.
Q. Okay.
And you also said that you reviewed a configuration file. Is that something that was produced in Exhibit 5?
A. Yes, I believe it's in here.
Q. And how did what was contained in the exhibit file confirm for you that the source code corresponded to what was described in Exhibit 2?
A. The schema for it.
Q. Excuse me?
A. The schema for the configuration file contained the elements described in this document.
Q. So Exhibit 2 describes the configuration file, and -- is that correct?
A. Indirectly, yes. If you look at each of the capabilities that you can configure, that's what you'd be looking for in the schema.
Q. So what -- what do you mean by schema of the configuration?
A. The structure of it. Did it have -- you know, did it have the element set present that would match this.
Q. So you made sure that the configuration file had certain -- had a certain structure that was reflected in

Page 94

what was described in Exhibit 2?
A. Yes.
Q. Did you confirm, as well, that on a --
Excuse me. Let me strike -- let me rephrase.
Did you also confirm that the source code would interact with the configuration file in a manner described in Exhibit 2?
A. No, we did not.
Q. So is it fair to say, then, you reviewed the configuration file to make sure that the structure of the configuration was similar to what was described in Exhibit 2 and you reviewed the time stamps in the source code archive to ensure that it was in the same time frame; is that -- as when Exhibit 2 was prepared?
MR. KING: Objection, form.
Q. BY MR. LIN: You may answer.
A. Yes.
Q. Okay.
Now, do you have any personal knowledge that Exhibit 2 describes a product that was released?
A. I do have some personal knowledge, yes.
Q. What's the extent of that personal knowledge?
A. When I was in Novell and we were interacting with Aventail, we had to do some setup and work with them, so -- I can't attest that this exact one I worked on, but I

Page 95

can attest that something that approximated this was released.
Q. So when you worked at Novell you acquired a released version of Aventail software; is that correct?
A. Yes.
Q. And while you were at Novell did you have access to Aventail confidential information or source code?
A. I don't believe we had access to the source code. We had access to some confidential information, the sharing of -- of design documents.
Q. Was Aventail under nondisclosure agreement with Novell before February of 2000?
A. I believe so.
Q. And can you describe the extent to which you tested the Aventail software while you were at Novell?
A. Yeah. We tested the software against -- against our SOCKS server for interoperability. We also tested it against our own network client as another LSP provider, so that the two could cooperate simultaneous.
Q. So Aventail Connect is capable of communicating with SOCKS servers other than Aventail's SOCKS server?
A. It was in -- at that time.
Q. It was not?
A. It was at that time.

Page 96

Q. At the time. Okay.
And do you have any personal knowledge of the -- any sales of Aventail Connect Version 3.1?
A. I do not.
Q. Do you have any personal knowledge of any offers for sale of Aventail Connect Version 3.1?
A. No, I do not.
Q. Do you have any personal knowledge of any public uses of Aventail Connect Version 3.1?
MR. KING: Objection, form.
THE WITNESS: During that time frame?
Q. BY MR. LIN: Yes.
A. No, no firsthand.
Q. Okay. Thank you.
Do you have any personal knowledge of any public disclosures of Aventail Version 3.1 prior to 2000?
A. Not -- well, no. You're -- no, I do not.
Q. Let me just ask the previous question again. Do you have any personal knowledge of any public disclosures of Aventail Version 3.1 prior to February 2000?
A. Not public.
Q. Okay. Thank you.
I'd like to direct your attention to Exhibit 3.
And did you prepare Exhibit 3?

Page 97

A. No, I did not.
Q. Have you seen Exhibit 3 before?
A. Yes, I have.
Q. And when did you first see Exhibit 3?
A. When we were pulling the information that we were being subpoenaed on.
Q. So you haven't seen Exhibit 3 prior to 2007; is that correct?
A. That is correct.
Q. And do you have any personal knowledge of who had custody of Exhibit 3 from the time it was prepared until the time you joined Aventail?
A. Not from when it was first prepared, but from when I joined. That would be Scott Boggan.
Q. But you don't have any personal knowledge as to who had custody of this document from when it was first prepared until when you joined Aventail?
A. I do not.
Q. And do you have any personal knowledge as to when Exhibit 3 was first published?
A. I haven't -- no, not firsthand.
Q. And did you undertake to verify the accuracy of the contents of Exhibit 3 with respect to any source code?
A. Yes, we did.

Page 98

Q. And when did you do that?
A. In December of 2007.
Q. And who did you speak with to determine that the contents of Exhibit 3 were consistent with the source code?
A. Bill Perry.
Q. And is Bill Perry still with SonicWALL?
A. Yes.
Q. And how much time did you spend comparing the contents of Exhibit 3 with the source code for Aventail ExtraWeb Server 3.2?
A. I spent less than a day.
Q. Less than a day.
And do you know approximately how many files are associated with ExtraWeb Server Version 3.2?
A. Well, I might now. Probably somewhere between -- maybe roughly 3,000 or so. I don't know the exact breakdown between the two. Some -- some of the code is shared.
Q. And did you review all 3,000 files of source code with Bill Perry?
A. I did not.
Q. Which source code files did Bill Perry write?
A. I don't know which ones.
Q. What was the extent of Bill Perry's involvement in developing the source code for ExtraWeb Server 3.2?

Page 99

A. I don't -- I don't know the magnitude of it. He is one of the founders.
Q. And did you do a page-by-page review of Exhibit 3 in connection with the source code?
A. I did not do page-by-page. I did samplings with Bill.
Q. And did you select the samplings of Exhibit 3 to compare with the source code?
A. Bill selected them.
Q. And approximately how many pages did you sample out of Exhibit 3 to compare with the source code?
A. I'd say roughly about one-third.
Q. One-third? Okay.
And when you identified a portion of Exhibit 3 that you wanted to compare with source code, how did you compare that portion of Exhibit 3 with the source code?
A. We used the same strategy. We used the configuration files to match up, you know, the user interface material with the actual structure of the configuration files.
Q. So you compared the structure of the configuration files. Did you also undertake to look at source code that might interact with the configuration files to perform a certain function?

Page 100

A. I did not.
Q. And do you have personal knowledge of whether Exhibit 3 accurately describes a product that was released?
A. I do not have personal knowledge.
Q. Do you have personal knowledge of any sales of ExtraWeb Server Version 3.2?
A. Not -- no, not direct.
Q. Do you have personal knowledge of any offer for --
Excuse me. Let me re -- restate that.
Do you have any personal knowledge of any offers for sale of Aventail ExtraWeb Server Version 3.2?
A. I do not.
Q. Do you have any personal knowledge of any public use of Aventail ExtraWeb Server Version 3.2?
A. I think so. I know of customer sites that I believe were running this when I joined the company.
Q. Do you have personal knowledge as to when those customer sites began using Aventail ExtraWeb Version 3.2?
A. I do not.
Q. Do you have any personal knowledge as to any public disclosure of Aventail ExtraWeb Version 3.2?

Page 101

A. Only in the form that it was at sites that were -- had bought it commercially.

Q. But you don't know when those sites first started using ExtraWeb Version 3.2; is that correct?

A. I do not.

Q. And you don't know when those sites first --

Excuse me. Let me restate that.

And you don't know whether any of the sites used ExtraWeb Version 3.2 prior to February of 2000; is that correct?

A. I do not.

Q. So for Exhibits 2 and 3, you don't have any personal knowledge as to anyone using these products prior to February 15, 2000; is that correct?

A. Not for commercial sale. I do in that we used it in our own development with Aventail.

Q. But not in public use; is that correct?

A. But not in public use.

Q. Okay. Thank you.

Do you have any personal knowledge as to how source code was maintained at Aventail prior to your joining Aventail in 2003?

A. I do not.

Q. And your experience with CVS, which is the repository for source code, is between 2003 and 2004; is

Page 102

that correct?

A. With Aventail, yes.

Q. Do you know when Microsoft first contacted SonicWALL in connection with the litigation with VirnetX?

A. I do not.

Q. Do you know whether Microsoft contacted SonicWALL in connection with the litigation with VirnetX?

A. I do not.

Q. Have you ever seen a subpoena that Microsoft sent to SonicWALL in connection with the litigation with VirnetX?

A. I may have.

Q. Do you know of any meetings between Microsoft and SonicWALL in connection with the litigation with VirnetX?

A. I do not.

Can I clarify that?

Q. Yeah, please.

A. How about a -- a representative of -- of Microsoft?

Q. Yes, that would include representatives from Microsoft, including their counsel.

A. I know of one where they were asking for information.

Q. Can you describe that meeting?

Page 103

A. Briefly. We were talking, I believe, to Tom, and Tom was clarifying the subpoena as to what -- essentially what they were looking for.

Q. Do you know when this meeting took place?

A. I believe it was November of 2007. I'm not positive about that.

Q. And in what regards did Microsoft or attorneys for Microsoft clarify what they were looking for in the subpoena?

A. They described our products. They knew of some of our products, specifically the ExtraNet and Connect, if I remember, and possibly ExtraWeb, and we discussed sort of the clarifications of what, you know, roughly those products did, and then they asked for -- or I think it might have been just Tom. I think it was Tom, asked for, you know, the kinds of information like, Gee, yeah, get me the -- the information on these, and that's where we kind of defined the scope with -- with Laurel on what it was we were -- they were looking for.

Q. Did this conversation include discussions about source code, Aventail source code?

A. Yes, it did, at the time.

Q. And what was said regarding Aventail source code?

A. That we could produce the source code.

Page 104

Q. And did SonicWALL produce the source code to Microsoft?

A. I believe so, but I -- I don't know when. I wasn't party to that.

Q. Do you know if Microsoft was given access to SonicWALL source code?

A. I do not.

Q. And when did you first gather the source code for production in response to Microsoft's subpoena?

A. In December of 2007.

Q. And is it your understanding that source code was actually provided to Microsoft in December of 2007?

A. I don't believe it was, but I -- I'm not the one who would provide it.

Q. Do you know when the source code was first provided to Microsoft?

A. I believe it was recently.

Q. How recently?

A. Within the last couple months.

Q. Okay.

Is it correct to say that Aventail Connect is software that runs on a computer?

A. Yes, it is correct.

Q. And I'm referring to Aventail Connect Version 3.1.

Page 105

A. Yes, that is correct.
Q. Is it correct to say that Aventail Connect Version 3.1 runs on a client computer?
A. That is a more precise.
Q. Is it correct to say that Aventail Connect does not always make a connection directly between the client computer and the remote host?
A. Yes, that is -- it never makes a direct connection.
Q. And is it okay with you if I also refer to remote host as a target computer?
A. Yes.
Q. Will you understand what I'm saying?
A. Yes.
Q. Okay.
A. As opposed to a VPN server?
Q. Okay.
Is it correct to say that Aventail Connect is specifically designed to operate only for TCP/IP communication?
A. That is incorrect.
Q. And in what way is it incorrect?
A. It could pass UDP traffic, as well.
Q. Okay.
Is it correct to say that for connections

Page 106

that are redirected to a SOCKS server, that Aventail Connect does not establish a direct connection between a client computer and the target computer?
MR. KING: Objection to form.
THE WITNESS: Yes, technically that is correct.
Q. BY MR. LIN: Is it correct to say that Aventail Connect establishes a connection between the client computer and the Aventail SOCKS server software?
A. That is correct.
Q. Is it correct to say that there's a separate connection established between the Aventail SOCKS server software and the target computer?
A. That is correct.
Q. Now, does Aventail Connect take any action in the absence of an application requesting a connection?
MR. KING: Objection, form.
THE WITNESS: Can you -- yeah. Maybe you could clarify that to me.
Q. BY MR. LIN: Okay.
What does Aventail Connect respond to?
MR. KING: Objection, form.
THE WITNESS: It responds to -- in this -- circa this era, it responds to WinSock requests.
Q. BY MR. LIN: And where are those WinSock

Page 107

requests -- where do those WinSock requests originate from?
A. In the client application.
Q. Okay.
So in the absence of a WinSock request from a client application, does Aventail Connect do anything?
A. No.
Q. What precisely does Aventail Connect do in response to a DNS request?
A. It interprets the -- the type of request, specifically looking for a name or an address --
And address could be a form of a name here.
Q. Okay.
A. -- that matches the configured redirection rule set on the client. If it matches, it forwards the request over a SOCKS connection to the SOCKS server to be resolved.
Q. Okay.
And does Aventail Connect do anything after that in the absence of any request from the application?
A. It caches the response as a handle, to be used in a subsequent WinSock request at an unknown point in time.
Q. And could a subsequent WinSock request include a connection request from the application?
A. Yes.

Page 108

Q. And what precisely does Aventail Connect do in response to receiving a connection request?
A. It looks to see if the IP address of the target server matches a cached handle that it's resolved it against its redirection set.
Q. So could I direct your attention to Exhibit 2. It's going to be Page 11. It's also Bates stamped AVEN 00000015.
A. You said Page 11?
Q. Yes.
A. Okay.
And what -- what was the rest of it?
Q. I was also identifying the Bates number, beginning in 015 at the beginning of the page.
A. Yes, okay. Yes.
Q. So Point No. 1, is that describing what Aventail Connect does in response to a DNS request?
A. Yeah, that -- it approximates it, yes.
Q. So the first -- first point, in summary, says that if the host name matches a local domain stream or does not match a redirection rule, then Aventail Connect passes the name resolution query through the IP -- TCP/IP stack, correct?
A. Yes, technically to whoever the next provider is.

Page 109

Q. And what is a local domain stream?
A. I believe it's the DNS domain you're a member of, that the client system is a member of.
Q. And what does it mean to not match a redirection rule?
A. Ah. It means that the name that is being looked up is not a name that has been programmed for redirection into the VPN.
Q. Why would you program a name for redirection to the VPN?
A. Because the system actually operates on names rather than IP addresses. It treats IP addresses like names.
For example, a host address or a subnet is also a form of a name. A DNS server's a name -- I mean, a DNS, either qualified fully or non, are names.
Q. Okay.
And if you turn to the next page, Page 12.
Does the first bullet on Page 12 describe what Aventail Connect does if a destination host name matches a redirection rule?
A. Yes, that's -- that's approximately what happens.
Q. And Aventail Connect creates a false DNS entry, correct?

Page 110

A. Yes.
Q. And what is a false DNS entry?
A. You know, I don't recall the exact structure. It's a -- it's a tag that we were using to subsequently recognize later on resolution.
Q. Does a false DNS entry correspond to the computer address of the target computer?
A. I believe it is populated by the -- by it, but it doesn't contain it at first.
Actually, let me clarify that a little more. It's -- it's false in the sense that the server knows the actual real address and that the proxy connection itself is going to be bound to it, and so we create a -- kind of a fake -- a fake address.
Q. Okay.
But that doesn't necessarily include the computer address of the target computer; is that correct?
A. You know, my memory's a little faulty. I don't believe it has the actual address of the target.
Q. Okay. Thank you.
So let's say, for example, the application has submitted a DNS request that matches a redirection rule. What is the next step the application will take to initiate a connection with the target computer?
And by "application" I'm talking about the WinSock application.

Page 111

A. Right.
So the -- this false entry, what happens there is we've created essentially an alias IP address, and I believe it's in the net2 namespace, which is not -- not allocated so we kind of stole it. So --
Q. Okay.
A. So, in other words, we create -- they're like NAT -- are you familiar with NAT?
Q. I'm not.
A. Okay.
So we create an address on the local side that actually is going to end up becoming bound to the remote address, right? Indirectly through the connection going from Connect proxy to the server. The server knows the real address associated with that -- that proxy -- it's like a -- yeah. That TCP connection coming in from the client's associated with remote address.
Q. Mm-hmm.
A. On the client side we associate a fake address back to the application.
Q. Okay.
A. We resolve it.
When the application comes through and initiates some form of a connect method, like Connect, let's

Page 112

say, for TCP, right, the address that they're connecting to is one of our false addresses, that we recognize and then look up in the table which T -- or who that's associated with and place the SOCKS connection back to the server.
Q. What do you mean, "who that's associated with"?
A. What -- what resolution that was associated with.
Q. What do you mean by "what resolution that was associated with"?
A. So if you -- if you translate a name, right, that we resolve via the SOCKS server, we get an imaginary, if you were, IP address that we've created for it, right? We reassociate that and pass it back through to the SOCKS server, who then looks up and says, Oh, this fake address on the client side is really associated with this actual target host.
Q. So you're saying the DNS resolution takes place at the SOCKS server; is that correct?
A. Yes. The actual DNS resolution takes place at the SOCKS server.
Q. Is the false DNS entry associated with anything that the SOCKS server might resolve?
A. Yes.
Q. And the purpose of that is to identify which

Page 113

SOCKS server will be used to redirect the connection; is that correct?
A. No. It's to identify what the target host is we're supposed to proxy to.
Q. So I believe you were in the process of describing what happens when the application requests a connection host, so you were saying that the application tries to connect to this false address; is that correct?
A. That's correct.
Q. And then what happens after that?
A. The Connect proxy intercepts that request, realizes that it's an IP address that was fabricated for the SOCKS server, and establishes the new SOCKS connection, passes that through to the server. The server, of course, now associates that with the real address.
Once that's all done, then we go ahead and pass the traffic on the connect coming through, which in TCP's case would be a TCP send.
Q. But that would only be in response to the application sending data; is that correct?
A. That's correct.
Q. Now, does the connection request contain a domain name?
A. It does not.
Q. The application -- the connection request

Page 114

from the application includes a computer address; is that correct?
A. It does.
Q. Does Aventail Connect respond to standard DNS requests?
A. Yes. It participates in the resolution of standard DNS requests when those are in the re -- when their name's in the redirected rule set.
Q. Does Aventail Connect require the DNS request from the application to be formatted in any particular way?
A. No, any standard DNS is -- is allowed.
Q. Does Aventail Connect modify the DNS software that is part of the Microsoft operating system?
A. It does not.
Q. Does Aventail Connect remove any DNS software that is part of the Microsoft operating system?
A. It does not.
Q. Does Aventail Connect disable the DNS software that is part of the Microsoft operating system?
A. It does not.
Q. Is the DNS request a standard IETF DNS request?
A. Yes.
Q. Does Aventail Connect's response to a DNS request ever include initiating a TCP/IP connection to the

Page 115

target computer?
A. No.
Q. Does Aventail Connect's response to a DNS request ever include initiating a VPN connection to the target computer?
A. Repeat that again.
Q. Does Aventail Connect's response to a DNS request ever include initiating a VPN connection to the target computer?
MR. KING: Objection, form.
THE WITNESS: No.
Q. BY MR. LIN: Do the redirection rules associated with Aventail Connect reside on the client computer?
A. Yes.
Q. Does the use of Aventail Connect require a user to configure the redirection rules on a client computer?
MR. KING: Objection, form.
THE WITNESS: It requires an administrator or a user to.
Q. BY MR. LIN: Without a user configuring the redirection rules, will Aventail Connect be connected?
A. It will be passive.
Q. Passive.

Page 116

So if an application request matches a redirection rule, is a new connection to the SOCKS server created?
A. Can you repeat that? I'm -- you're so specific.
Q. Sorry.
A. It's okay.
Q. If an application request matches a redirection rule, is a new connection to the SOCKS server created?
MR. KING: Objection, form.
THE WITNESS: Yes.
Q. BY MR. LIN: So for each new application request a separate connection is made to the SOCKS server; is that correct?
A. Correct.
Q. After Aventail Connect makes a connection to the SOCKS server, does the SOCKS server then make a new connection to the remote host?
A. Yes.
Q. If Application A sends data on a specific connection to the SOCKS server, then will the data always go on -- to the same remote host?
A. Application A.
MR. KING: Objection, form.

Page 117

THE WITNESS: Repeat that, please.
Q. BY MR. LIN: If an application sends data on a specific connection to the SOCKS server, will the data always go to the same remote host?
A. Yes.
Q. Can it ever go anywhere else?
A. No.
Q. If another application -- let's call it Application --
A. Let me -- I need to clarify that. Can a UDP --
No, no. That's true. Never mind. The answer was correct.
Q. Okay.
If another application, let's call it Application B, sends data on another specific connection to the SOCKS server, will that data always go to the same remote host?
A. I believe so.
Let -- let me see if I got that right. So if the application initiates a connection with a different target --
Q. If a different application.
A. If a different -- even the same, but -- if an application initiates with a different target, will it

Page 118

always go over the same SOCKS connection and the associated same proxy connection to that --
Q. Go ahead, answer that question.
A. Yes.
Q. So if you have a second application that has another specific connection to a SOCKS server, and it's always -- it's routing data to a remote host, will the data from Application B always go to the same remote host?
A. To Target B?
Q. Yeah.
A. Yes.
Q. Okay.
So would you agree with me that there's no routing occurring -- occurring in the SOCKS server?
A. Yes.
Q. Does Aventail Connect require any special functionality on the target computer?
A. No.
Q. Are there any specific capabilities that the target computer must have?
MR. KING: Objection, form.
THE WITNESS: None that I'm aware of.
Q. BY MR. LIN: Does Aventail Connect require the target computer to be able to perform encryption?
A. No.

Page 119

Q. Does Aventail Connect require the target computer to be able to perform decryption?
A. No.
Q. Does Aventail Connect require the target computer to be able to form part of a VPN?
A. No.
Q. Are you familiar with the concept of a tunnel?
A. Yes.
Q. And what is your understanding of what a tunnel is?
A. A tunnel is used in different contexts. In a routed context, it's used to encapsulate packets that are going through to be routed. In a proxy context, it's designed to encapsulate data one to one with a target.
Q. And we've already established that Aventail is not in a routed context; is that correct?
A. That is correct, with Connect and SOCKS.
Q. Does Aventail Connect tunnel IP packets within IP packets?
A. Yes.
Q. Can you explain that?
A. The SOCKS encapsulation is flowing over TCP/IP. Then the application traffic, which also has IP, could be TCP or UDP, is being transmitted as packets

Page 120

encapsulated within SOCKS. So IP in IP is true.
Q. Does Aventail Connect tunnel network layer --
A. You know what, let me -- actually, let -- hold on a second. Let me think about that a little more.
No, I answered that wrong. I'm sorry. I was thinking of tunneling technology.
Q. Can I ask that question again?
A. Yes, please answer it again -- ask it again.
Q. Does Aventail Connect tunnel IP packets within IP packets?
A. No.
Q. Does Aventail Connect tunnel network layer packets within network layer packets?
A. No.
MS. BUCKNER: Counsel, can I just clarify exactly what you're talking about in terms of the product that you're asking about currently?
MR. LIN: We're talking about Aventail Connect.
MS. BUCKNER: And the version is?
MR. LIN: Version 3.1.
MS. BUCKNER: Okay. Because currently SonicWALL has a product which is called the Tunnel -- Aventail Tunnel.
MR. LIN: Okay.

Page 121

MS. BUCKNER: I don't even know if we're branding it Aventail Connect Tunnel now, but I just want to make sure that we're not currently talking about SonicWALL's product, we're talking about the previous --
MR. LIN: Right.
MS. BUCKNER: And would you restate, I guess, the version that you're asking about specifically?
MR. LIN: Sure. We're asking about Aventail Connect Version 3.1.
MS. BUCKNER: Thank you.
MR. LIN: Thanks for the clarification. Appreciate it.
Q. And you understand that we've been talking about Aventail Connect Version 3.1; is that correct?
A. Yes. I -- I was thinking of one of our other products which does that, but that's the reason I had to retract that.
Q. Thank you.
In the Aventail version -- in Aventail Connect Version 3.1, what is being encapsulated within the packets?
A. The payload of the application traffic.
Q. Is there anything else?
A. Well, and it's also framed with, you know, the encryption.

Page 122

Q. So the payload packet has encryption information and the actual encrypted content; is that correct?
MR. KING: Objection, form.
THE WITNESS: Yes. The payload is encapsulated in SOCKS, and within SOCKS encryption optionally, although typically employed, is also present with, you know, the necessary cryptography wrapper.
Q. BY MR. LIN: So an Aventail connection with the SOCKS server is not always encrypted; is that correct?
A. It's possible to configure it for non -- nonencryption.
Q. So it's correct that the connections between Aventail Connect and a SOCKS server are not always encrypted?
A. That is correct.
Q. Do all connections made with Aventail Connect via the SOCKS server require authorization?
A. Yes.
(Discussion off the record.)
Q. BY MR. LIN: Actually, let me just turn back to something I was asking you about earlier, and was about the tunneling in Aventail Connect Version 3.1. Now, in the packets that are being sent between Aventail Connect and SOCKS, is the payload -- excuse me -- is the packet that's

Page 123

being encapsulated the same as the packet that's being encapsulated between the SOCKS server and the target computer?
MR. KING: Objection, form.
THE WITNESS: The application payload is the same.
Q. BY MR. LIN: Is -- if encryption is used between the Aventail Connect software and the SOCKS server, is the information being transmitted between the SOCKS server and the target computer also encrypted?
A. It's -- it's the -- whatever the plain text of the data was is being transmitted.
Q. So it's been decrypted; is that correct?
A. It's -- yes. The VPN decryption is done at the SOCKS server.
Q. So the payload between Aventail Connect and the SOCKS server is not the same as the payload between the SOCKS server and the remote host; is that correct?
A. The TCP payload is not the same between the SOCKS server and the SOCKS client. The application payload that's encapsulated inside it is encrypted normally.
Q. This is between the SOCKS client and the SOCKS server?
A. Correct.
Q. But it's not encrypted between the SOCKS

Page 124

server and the remote host; is that correct?
A. Not unless the application encrypted it.
Q. Okay.
What happens to the source and destination information between the two connections? And by "two connections" I mean between the SOCKS client, the SOCKS server, and between the SOCKS server and the remote host.
A. At the network layer, at the IP layer?
Q. Yes.
A. The source and destination IP addresses are the actual IP address of the client, the real adapter address, whichever it's gone out on --
Q. Mm-hmm.
A. -- and the IP address that the SOCKS client contacted the SOCKS server on.
Q. Okay.
A. And between the SOCKS server and the target server, it is the IP address of the adapter that we are initiating from on the SOCKS server and the IP address of the target server.
Q. Okay. Thank you.
So I'd like to --
Is the Aventail Connect source information transmitted to the target?
A. No.

Page 125

MR. KING: Objection, form.
Q. BY MR. LIN: So I believe earlier you testified that all connections made with Aventail Connect via the SOCKS server require authorization; is that correct?
A. That is correct.
Q. Can you please turn to Exhibit 2, Bates No. AVEN 0000052.
Actually, I may have given you the wrong page.
Right. So that's Page 48 of Exhibit 2, correct?
A. Yes, administrator's guide 48.
Q. Do you see the table at the very top?
A. Yes.
Q. Do you see in the second row, second column, it states, "<Null Auth> indicates no authentication module will be used"?
A. Yes.
Q. Is this consistent with your testimony that all connections made with Aventail Connect via the SOCKS server require authorization?
A. Yes.
Q. And how -- how is this consistent with what's shown on Page 48?
A. This is authentication. Authentication is

Page 126

authenticating identity. Authorization is authorizing it to pass to a target.
Q. And how does -- how does Aventail Connect require authorization to connect to the target?
A. The SOCKS server enforces the authorization through access control rules.
MS. BUCKNER: I think there might be some movement now where we might be going into some SonicWALL confidential information.
MR. LIN: Okay.
MS. BUCKNER: So I've just appraised Gary of noting to me when there are pieces that may be in our current product.
MR. LIN: Okay.
MS. BUCKNER: And he's just notified me that as we're moving forward --
THE WITNESS: We might be.
MS. BUCKNER: -- this might be a time where that may be at issue.
MR. LIN: Okay. I understand.
I'll try to restrict my questions to the document.
MS. BUCKNER: Thank you.
Q. BY MR. LIN: Can you show me where in this document the access controls are described?

Page 127

A. Oh, wait a second. This is the --
Oh, it won't be in this document.
Q. Is there another -- would it be in Exhibit 3?
A. Yes.
Q. Can you show me where in Exhibit 3 access controls are discussed?
A. Yeah, the first example's going to be on AVEN 00000143. There's a row that says "Deny, Anywhere, Anywhere, Anyone, Times Any." That would be an access control rule.
That would be a pretty Draconian one but . . .
Q. Okay. Thank you.
In the context of Aventail Connect Version 3.1, what is a channel?
A. Where did you see that?
Q. It's not in the documents. That's just the question.
A. My understanding of the channel would be the TCP connection, but that -- that's how I've heard of it referred to.
Q. Is the TCP connection between the client and the SOCKS server?
A. Yes.
Q. In this context and based on your

Page 128

understanding, is a channel a network?
A. No, it's a secure pathway over a network.
Q. Okay.
And you understand that different people might have different interpretations of what a VPN is?
A. Yes.
Q. Do you understand that different people might have different interpretations of what a tunnel is?
A. Yes.
Q. And do you understand that your definition of a VPN might be different than someone else's definition of a VPN?
A. Yes.
Q. Do you understand that your definition of a tunnel might be different from someone else's definition of a tunnel?
A. Yes.
Q. Okay.
If I could have you turn back to Exhibit 2.
If you could flip to Bates No. AVEN 00005120.
A. 5120?
Q. I'm sorry. 120. 00000120.
A. Okay.
Yes, I'm there.
Q. Do you see the definition of "Virtual Private

Page 129

Network" at the top?
A. I do.
Q. Is this Aventail's definition of a virtual private network?
A. It is.
Q. Is this also your definition of a virtual private network?
A. Yes.
Can I clarify that once?
Q. Yeah, please.
A. Yes, with respect to this -- with Connect V3.1.
Q. So you think this definition of VPN on Page 116 of Exhibit 2 is a correct definition of VPN with respect to this Aventail Connect 3.1?
A. I do.
Q. Do you believe that is an accurate definition of VPN for other products other than Aventail Connect 3.1?
A. In principle, yes.
Q. Now, you testified earlier --
Strike that last question.
Is your previous testimony about what a channel is consistent with "channel" as it's used in the definition of VPN on Page 116 of Exhibit 2?
A. I believe it is.

Page 130

Q. Is the DNS server part of the Aventail product line?
A. No.
Q. Is the DNS mentioned in the Aventail Connect documents, such as Exhibit 2 and Exhibit 3, a DNS server that's produced by Aventail?
A. No.
Q. Is the DNS that's mentioned in Exhibits 2 and 3 simply any standard DNS service?
A. Yes, with respect to meeting IETF standard protocol.
Q. Yes.
Is a DNS proxy server part of the Aventail product line?
MR. KING: Objection, form.
THE WITNESS: Let me think of that.
No, not a general-purpose DNS proxy server.
Q. BY MR. LIN: Is it reasonable to identify some part of Aventail Connect as a DNS proxy server?
A. Yes.
Q. And which part would that be?
A. The part that translates them into fake entries.
Q. And this runs on the client computer; is that correct?

Page 131

A. Correct.
Q. It does not run on the target computer?
A. It does not.
Q. And it does not run on the SOCKS server computer; is that correct?
A. Well, actually, I can't ask for the target computer, but -- it does not run on the SOCKS server.
Q. And the redirection rules reside on the DNS proxy server; is that correct?
A. They reside on the client.
Q. Okay.
And which is --
A. The -- they reside as a component of Connect.
Q. Is the DNS proxy server functionality separate from the redirection rules?
A. You're referring to the DNS resolution Connect does?
Q. Yes?
MR. KING: Objection, form.
THE WITNESS: No, the redirection rules are -- are part of the spoof translations that it operates on.
Q. BY MR. LIN: And, sir, what is your definition of a tunnel in the context of Aventail Connect Version 3.1?

Page 132

A. It's -- it's a form of a channel.
Q. Any particular --
A. It's a one-to-one mapping of an application connection to a proxied connection to a target server.
Q. Okay.
Is it possible for an application to send a nonstandard domain name to Aventail Connect?
A. Yes.
Q. And how does Aventail Connect respond to a nonstandard domain name?
A. It looks to see if it's a WINS name, which is a Microsoft proprietary resolver, and it attempts to resolve it via WINS.
Q. Okay.
Aside from a WINS name, can Aventail Connect respond to any other nonstandard domain name?
A. No.
Q. And can you explain further what Aventail Connect Version 3.1 does with a WINS name?
Maybe we should start, what is a WINS name?
A. Microsoft has its own proprietary name service, called WINS. It's integrated with their networking system. And the WINS name is forwarded to the SOCKS server, just like a DNS name would be. And the SOCKS server is the one who tries to discriminate it as being WINS.

Page 133

Q. So in what context would an application use a WINS request?
A. A file share.
Q. Is there anything else?
A. Mostly it's Microsoft applications and older ones that use it. I'm not familiar with all of them.
Q. Okay.
Does the fact that Aventail Connect is processing a WINS name mean that Aventail Connect is going to create a secure connection to the SOCKS server?
A. Yes.
Q. Is that set forth in a redirection rule?
A. WINS can be part of a redirection rule.
Q. Is it necessarily part of a redirection rule?
A. It doesn't have to be.
Q. So WINS could be a request on the local domain; is that correct?
A. Correct.
Q. And in that context, the connection is not proxied by the SOCKS server; is that correct?
A. That's correct.
Q. Okay.
Could we go off the record, please.
THE VIDEOGRAPHER: Going off record. The time is 2:41 p.m.

Page 134

(Discussion off the record.)
(Short recess.)
THE VIDEOGRAPHER: This marks the beginning of Tape No. 3. Back on the record. The time is 2:56 p.m.
MS. BUCKNER: Counsel, I wanted to state for the record that the source code was provided to defendant's counsel in response to the subpoena just this week, at the same time that plaintiff's counsel did receive a carbon copy of the letter that was sent to defendant's counsel requesting him to share the source code with plaintiff's counsel.
MR. LIN: Thank you.
MS. BUCKNER: Mm-hmm.
Q. BY MR. LIN: Now, if I told you that a VPN required routing, would Aventail Connect 3.1 still be part of a VPN?
MR. KING: Objection, form.
THE WITNESS: Boy.
Routing -- where is the routing done?
Q. BY MR. LIN: The routing is done by the SOCKS server.
A. Yes.
Q. You testified earlier that the SOCKS server did not route connections from Aventail Connect. Do you recall that testimony?

Page 135

A. I do. The reason I said yes is that we have routing on the server, it can route -- I mean, we can establish routes for the outbound connection to the target using routing. It's not routing packets through the VPN.
Q. So your testimony is that the SOCKS server does not route packets through VPN?
A. That is correct.
Q. So if the V -- definition of VPN stated that packets need to be routed through the VPN, would Aventail Connect 3.1 still form part of a VPN?
A. No.
Q. And throughout your testimony we've been talking about Aventail Connect 3.1. I also understand that Exhibit 2 covers Aventail Connect Version 2.6.
A. Yes.
Q. What are the key distinctions between Aventail Version -- Aventail Connect Version 2.6 and Aventail Connect Version 3.1?
A. I do not know that.
Q. Would you turn to Exhibit 2, Page 10.
A. Yes.
Q. Do you see the third paragraph from the bottom?
A. Third, "For those platforms"?
Q. Excuse me. Third paragraph from the bottom,

Page 136

where it says, "The Aventail Connect 2.6."
A. Oh, excuse me, yeah. I didn't notice it was a paragraph.
Yes.
Q. Does that refresh your recollection as to what the differences between Aventail Connect 2.6 and Aventail Connect 3.1 might be?
A. Yes, I know what that means. So I -- if I see that I -- I would -- I'd have to speculate, but I -- I know what MultiProxy means.
Q. Okay.
So is it your testimony that what you testified to earlier would also apply to Aventail Connect Version 2.6?
A. I believe so.
Q. Okay.
Can you also look at Page 11 for me.
A. Yes.
Q. Do you see the third column of the table at the top, it says "Aventail Connect Version Installed"?
A. Yes.
Q. And Aventail Connect 2.6 is applied to operating systems that support WinSock 1.1.
A. Yes.
Q. Does that -- does that refresh your

Page 137

recollection as to any other differences there might be between Aventail Connect 3.1 and 2.6?

A. Well, I don't know the limitations of the WinSock 1.1. I'm not as familiar with WinSock 1.1 as WinSock 2. I can't answer that.

Q. Okay.

Do you know whether WinSock 1.1 also supports encryption?

A. Well, the Win -- the WinSock library itself doesn't have a notion of encryption. 1.1 or 2.0.

Q. Okay.

So while you were working at Novell with -- and you were experimenting with some of the Aventail Connect products, did you ever use WINS names as part of your testing?

A. I don't believe so.

Q. And can I ask you to turn to Exhibit 4, please.

A. Yes.

Q. Did you prepare this document?

A. I did not.

Q. Have you seen this document before?

A. Yes.

Q. When is the first time you saw this document?

A. When we were acquiring information for the

Page 138

subpoena.

Q. Was that in 2007?

A. Yes.

Q. So is it your testimony that you had not seen this document prior to 2007?

A. I may have seen it earlier, as -- but, you know, I don't -- I don't really recall.

Q. Do you have any personal knowledge as to who maintained custody of this document from the time it was created until the time you joined Aventail?

A. I only know who had it when I joined.

Q. So you had no personal knowledge as to who maintained custody of this document from when it was created --

A. I do not.

Q. -- until it was -- until you joined Aventail; is that correct?

A. No.

Q. Okay.

Do you have any personal knowledge as to when this document was published?

A. I do not.

Q. Can you personally vouch for the accuracy of Exhibit 4?

A. Not completely by myself.

Page 139

Q. Did you undertake to ensure that Exhibit 4 was complete and accurate?

A. Yes.

Q. And what did you do?

A. We used the same strategy as with the other two. We had a developer go through it, match it up.

I don't know all the criteria he used.

Q. Okay.

Did you review Exhibit 4 on a page-by-page basis and compare the features discussed therein with the source code?

A. I -- I did not. I sampled it only.

Q. And how long did you undertake to compare the contents of Exhibit 4 with what's in the source code?

A. This was less than a day.

Q. Okay.

And do you have any personal knowledge of any sales of the product described in Exhibit 4?

A. I don't. It's the same question as Exhibit 5.

Q. Okay.

A. I mean, 2. Excuse me.

Q. So is it your testimony that Exhibit 4 corresponds to the same product as Exhibit 2?

A. To the best of my knowledge.

Page 140

Q. Okay.

I'd direct your attention to Exhibit 6, please.

A. Yes.

Q. And Exhibit 6 is the same as Exhibit 7; is that correct?

A. I -- I believe so. I can't do a diff here but it looks like it is.

Q. Okay.

Have you seen this document before today, Exhibit 6?

A. I -- I might have. I don't -- I don't recall if we went through this particular part of the source.

Q. Did you write the source code that is in Exhibit 6?

A. No, I did not.

Q. Do you know what language the source code is written in?

A. Yes, C++.

Q. Do you have any experience developing C++ code?

A. I do.

Q. So you can read C++ code?

A. Not as well as I used to. Still somewhat.

Q. When was the last time that you personally

Page 141

developed C++ code?
A. 2001.
Q. Did you develop any source code for Aventail Connect Version 3.1 prior to February 15th, 2000?
A. No.
Q. And earlier we were talking about the concept of a tunnel. Does a tunnel exist between the SOCKS server and the target computer?
A. No.
MR. LIN: Okay. That's all I have.
MR. KING: All right. Let me ask a few follow-up questions, then.
THE WITNESS: Okay.

FURTHER EXAMINATION

BY MR. KING:
Q. I want to talk to you for a few minutes about your time at Novell.
A. Okay.
Q. Do you recall testifying that information exchanged between Novell and Aventail was done pursuant to nondisclosure agreements?
A. I was not a party to -- to the NDAs, but I believe they were in place, as we clearly were conveying confidential information.

Page 142

Q. Okay.
Did Aventail -- how did you obtain a copy of -- of the Aventail -- the Aventail product that worked with WinSock 2?
A. We exchanged our products directly with each other, development organization to development organization.
Q. How -- can you tell me more? How did that work?
A. I think they probably came on CDs, you know, that they would ship to us. I don't -- I'm trying to remember. I don't think we were transferring them over the Internet in that day, but we would take interim -- you know, interim builds.
I was not part of QA itself so I'm not sure what -- what happened after we thought it worked.
Q. Did you -- so did you personally use these -- these interim builds that arrived on CD?
A. I used -- yes, occasionally.
Q. Okay.
A. I mean, this wasn't a primary objective of mine, but yes. I was part of working with Aventail.
Q. Did you receive final builds from Aventail of their product?
Strike that.
Let me ask you a question. Did you receive

Page 143

the -- the Aventail -- the final build of the Aventail product that was com -- that was capable of using WinSock 2?
A. No, I don't -- I actually don't remember.
MR. LIN: Object to form.
Q. BY MR. KING: Okay.
When Aventail provided you with these interim builds, were -- was Novell supposed to keep the interim build confidential?
A. Yes.
Q. Do you have any sense as to when the first Aventail product that was -- Aventail VPN product that was compatible with WinSock 2 was actually released to the public?
MR. LIN: Object to form.
THE WITNESS: Compatible with WinSock 2. WinSock 2 is a client --
Oh. Any Novell product or with Aventail?
Q. BY MR. KING: Let me ask the question again.
A. Okay.
Q. This is sort of -- this is -- part of the problem is that it's -- it's a little bit clunky to refer to the first Aventail product that was compatible with WinSock 2, so maybe --
Let me ask you a question. Do you know the name of the first Aventail product that was compatible with

Page 144

WinSock 2?
MR. LIN: Object to form.
THE WITNESS: I don't recall if it was 2.6 or 3.1.
Q. BY MR. KING: Okay.
Was it one of those two products, though?
MR. LIN: Object to form.
THE WITNESS: Well, we were compatible in 1997 at an interoperable level with some version of Aventail.
Q. BY MR. KING: Okay.
A. I don't know which one.
Q. Okay.
Was it public knowledge that Aventail --
Strike that.
Was it public knowledge in 1999 that Aventail was building a Win -- WinSock 2 capable VPN client?
MR. LIN: Object to form.
THE WITNESS: I -- I believe that it was. I believe it was available, you know, public -- publicly disclosed on their Web sites, but I -- I cannot, you know, attest with absolute certainty that's true.
Q. BY MR. KING: Why do you -- why do you believe that it was publicly disclosed on their Web site?
MR. LIN: Object to form.

Page 145

THE WITNESS: In working with our biz dev people. I mean, you know, I don't -- I just recall it being like a product that they were going out and co -- well, doing whatever reference things with.

Q. BY MR. KING: When you -- you're talking about your interactions with your Novell biz dev people, right?

A. Yes.

MR. LIN: Objection. Leading.

Q. BY MR. KING: Do you recall -- I'm going to change subjects here for a second. Do you recall testifying that Aventail Connect 3.1 does not create a direct connection between the client and the ultimate target computer?

A. I do.

Q. What would you call -- if it's not a direct connection, what would you call the link between the client computer and the target computer?

MR. LIN: Objection. Leading, and form.

THE WITNESS: It's an indirect through a proxy.

Q. BY MR. KING: Can you describe that indirect link through a proxy for me?

MR. LIN: Objection to form.

THE WITNESS: Calls an intermediate system,

Page 146

who in turn calls the final target, and then links the two together through a forwarding relationship.

Q. BY MR. KING: Okay.

And is the VP -- is the SOCKS server the intermediate system that you just referred to?

A. Yes.

Q. Where does the VPN -- where is the VPN created in this scenario?

MR. LIN: Object to form.

THE WITNESS: It is created between the SOCKS -- I mean, the Connect client and the Connect server.

Q. BY MR. KING: So logically there is a VPN that sits between the Connect client and the target computer, even though the VPN doesn't actually connect to the target computer; is that right?

MR. LIN: Objection. Leading and form.

THE WITNESS: Yes, that is true.

Q. BY MR. KING: Let's take a look at Exhibit 2, the very last page, where the glossary resides.

A. Yes.

Q. It's Page 25 of -- of the glossary.

Actually, you know what, I think I have the wrong document. Let's take a look at Page 25 --

A. Of which --

MR. LIN: It's also in this document.

Page 147

MR. KING: All right. I see my problem.

Q. It's Page 116 of Exhibit 2.

A. Okay. Thank you.

Q. Too many glossaries in this world.

Do you see that -- the definition of VPN as "a secure channel used to transmit data over a public network"?

A. I do.

Q. Is any secure channel that transmits data over a public network a VPN?

A. No.

Q. Why not?

A. I would say that one is -- that is terminated by the two end points on the public network as the ultimate terminus is not a VPN.

Q. Can you give me some examples of that?

MR. LIN: Object to form.

THE WITNESS: Yes. For example, if you're doing e-commerce with a Web site directly, I would say that's not a VPN.

Q. BY MR. KING: Can you give me some other -- some other examples?

A. I think anytime applications are directly communicating with each other, right, not going through some kind of a secure intermediary, they're not a VPN.

Page 148

Q. What about a voiceover IP connection that's encrypted, would that be a VPN?

MR. LIN: Object to form.

THE WITNESS: If it's direct to the -- the other party, no.

Q. BY MR. KING: Okay.

Okay, that's -- that's all that I have for now.

MR. LIN: All right. We're good.

MR. KING: Okay. I think we're finished. Thank you very much.

MR. LIN: Thank you so much for your time.

THE WITNESS: Thank you, gentlemen.

THE VIDEOGRAPHER: This marks the end of Videotape No. 3 in the deposition of Gary Tomlinson. Going off the record. The time is 3:17 p.m.

(The videotape deposition of Gary Tomlinson was concluded at 3:17 p.m.)

---o---

Page 149

AFFIDAVIT

STATE OF WASHINGTON)
) SS.
COUNTY OF KING)

I have read my within deposition, taken on Friday, February 27, 2009, and the same is true and correct, save and except for changes and/or corrections, if any, as indicated by me on the "CORRECTIONS" flyleaf page hereof.

____
GARY TOMLINSON

SUBSCRIBED AND SWORN to before me this ________ day of _______________, 2009.

____
NOTARY PUBLIC in and for the State of Washington, residing at ______________. My commission expires _________________.

CERTIFICATE

STATE OF WASHINGTON)
) ss.
COUNTY OF KING)

I, the undersigned officer of the Court, under my commission as a Notary Public in and for the State of Washington, hereby certify that the foregoing deposition upon oral examination of the witness named herein was taken stenographically before me and thereafter transcribed under my direction;

That the witness before the examination was first duly sworn by me to testify truthfully; that the transcript of the deposition is a full, true and correct transcript of the testimony, including questions and answers and all objections, motions, and exceptions of counsel made and taken at the time of the foregoing examination;

That I am neither attorney for nor a relative or employee of any of the parties to the action; further, that I am not a relative or employee of any attorney or counsel employed by the parties hereto, nor financially interested in its outcome.

IN WITNESS WHEREOF, I have hereunto set my hand and seal this 13th day of March, 2009.

____
NOTARY PUBLIC in and for the State of Washington, residing at Redmond. My commission expires 04-6-10.

A

T

Electronic Acknowledgement Receipt

EFS ID:	9199805
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN
Receipt Date:	10-JAN-2011
Filing Date:	16-AUG-2007
Time Stamp:	16:45:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Examination support document	ExA.pdf	252523 208e777e0a8a148f6233da23ca4cc39da4b99010	no	8

Warnings:

Information:

2	Examination support document	ExB.pdf	2036326 a184d035037d4f979aa5c712fa7a1c4b9eb8bb43	no	39
Warnings:					
Information:					
3	Examination support document	ExC.pdf	762947 96751d6187bbe11180b7553ca6d9eeee90661679	no	21
Warnings:					
Information:					
4	Examination support document	ExD.pdf	1064850 18ba07d329b27cef9a7944c9d6e9b4e0e0e72b2c	no	34
Warnings:					
Information:					
5	Examination support document	F1.pdf	377631 fc54df0b5052010e6e112745ff4dc07ab72d9359	no	120
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
6	Examination support document	F2.pdf	495792 f37ab8c3b7912118800eeadfd6e296f5df9b6dc2	no	152
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
7	Examination support document	F3.pdf	442253 a6e52caf0ff3e6e0f18b75ba3f6a157f5a07f83b	no	132
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
8	Examination support document	F4.pdf	502114 c04a3fdb897de4046a2a53b66789c7eca1903a7c	no	171
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					

9	Examination support document	F5.pdf	416607 2433730241f7db4439b60acd967df497105925cf	no	126

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

10	Examination support document	F6.pdf	563388 d26b18847156185e767ead345c2d0ca5e4ca813c	no	192

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

11	Examination support document	F7.pdf	356719 8f4352574556224a349b0d6f4add2c0632a7416a	no	121

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

12	Examination support document	F8.pdf	596436 d5e8432f8da8fa13a71eed17b0a45c4bfb34ee4f	no	179

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

13	Examination support document	F9.pdf	449976 e8645f491348ddf9e3f6ce25f2913e02209c9b7a	no	132

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

14	Examination support document	F10.pdf	568806 38d433895856fd3351a9a344fc9da6a4fb35f5f7	no	168

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

15	Examination support document	F11.pdf	520664 6ed994875b698427582c74ac3c8f5cfbcf9cdd6e	no	154

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

16	Examination support document	F12.pdf	700893 331461341a66e84ee941cf3aced37994a2c737f6	no	204

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

17	Examination support document	ExG.pdf	1311128 8d5d31485b15136bbe049a4808ede4ee244ffcb6	no	49

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

18	Examination support document	ExE.pdf	466743 68771cc5e456f27d80cf6cab285e4b7052c2f730	no	33

Warnings:

Information:

19	Examination support document	ExH.pdf	1590887 3ad8ef90819cf98ff6f614d78cca3f1e5aa4b3c0	no	61

Warnings:

Information:

Total Files Size (in bytes):	13476683

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/839,987	Filing Date 08/16/2007	☐ To be Mailed

APPLICATION AS FILED – PART I

FOR	NUMBER FILED (Column 1)	NUMBER EXTRA (Column 2)	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
			TOTAL			TOTAL	

* If the difference in column 1 is less than zero, enter “0” in column 2.

APPLICATION AS AMENDED – PART II

AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	01/10/2011									
	Total (37 CFR 1.16(i))	* 1	Minus	** 20	= 0	X $ =		OR	X $52=	0
	Independent (37 CFR 1.16(h))	* 1	Minus	***3	= 0	X $ =		OR	X $220=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	**0**

AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write “0” in column 3.
** If the “Highest Number Previously Paid For” IN THIS SPACE is less than 20, enter “20”.
*** If the “Highest Number Previously Paid For” IN THIS SPACE is less than 3, enter “3”.
The “Highest Number Previously Paid For” (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/PATRICIA F. LEWIS/

Application Number	Application/Control No. 11/839,987	Applicant(s)/Patent under Reexamination LARSON ET AL.	

Document Code - DISQ	**Internal Document – DO NOT MAIL**

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 01/10/11	**This patent is subject to a Terminal Disclaimer**	

Approved/Disapproved by:

Felicia D. Roberts

11/679,416

U.S. Patent and Trademark Office

Electronic Patent Application Fee Transmittal

Application Number:	11839987
Filing Date:	16-Aug-2007
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer./Kerrie Jones
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
	Total in USD ($)			**180**

Electronic Acknowledgement Receipt

EFS ID:	9446724
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN
Receipt Date:	15-FEB-2011
Filing Date:	16-AUG-2007
Time Stamp:	14:18:37
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	644
Deposit Account	501133
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	NPL Documents	1FOA0016.pdf	322936 afb8b1922dd09994b7dd951119c7359457318144	no	9
Warnings:					
Information:					
2	NPL Documents	1FOA0037.pdf	256341 79b8b6386825b06537adbdeb1249272dc7a7e88c	no	8
Warnings:					
Information:					
3	NPL Documents	1NFOA0012.pdf	251995 184fd07ab4ed6fc5bad9776525faf34b32474aff	no	6
Warnings:					
Information:					
4	NPL Documents	1NFOA0016.pdf	358100 beec30a5f5ebc1538521c4eb1548c73a3835a044	no	10
Warnings:					
Information:					
5	NPL Documents	1NFOA0037.pdf	274457 a61f5be1b26fd5912d159b61ac05ad4f6286a950	no	7
Warnings:					
Information:					
6	NPL Documents	1NFOA0038.pdf	198309 b29566c7f91ad7f4434c52fe82e131ad1f1bd830	no	6
Warnings:					
Information:					
7	NPL Documents	1NFOA0039.pdf	157064 c81a3db8199ddeebe0f547d41ce8ec9ce5434b7b	no	4
Warnings:					
Information:					
8	NPL Documents	1NOA0040.pdf	360294 dc31da9b9e57c03c572011f5af1bd188e9e0db87	no	7
Warnings:					
Information:					
9	NPL Documents	1NOA0041.pdf	667120 c190059565f36fee3af8bb3c823e40a24e15acc5	no	13
Warnings:					
Information:					

10	NPL Documents	1NOA0042.pdf	453844 28e5d2f82edaee3484af1995d4c230731b52c85f	no	9
Warnings:					
Information:					
11	NPL Documents	1NOA0044.pdf	724222 777ae7755a783cced396d2e903d19baaf11d364f	no	18
Warnings:					
Information:					
12	NPL Documents	1NOA0057.pdf	754386 9a900f865150257d219ada8f208b00896c771832	no	16
Warnings:					
Information:					
13	NPL Documents	1NonFinalOA0015.pdf	231236 9831e8313ae51904786ae063ab0a5ef62aa02154	no	6
Warnings:					
Information:					
14	NPL Documents	1NonFinalOA0044.pdf	416656 5cf8d286e00efcb7e93d0e7e13fe12f4453b3dbf	no	13
Warnings:					
Information:					
15	NPL Documents	1NonFinalOA0057.pdf	170178 a8e6797a7ffef393155e12f9ff964265558d9498	no	5
Warnings:					
Information:					
16	NPL Documents	1NonFinalOA0063.pdf	295823 e6ec72f6b38b0571d24577c904f996b6bfe05585	no	7
Warnings:					
Information:					
17	NPL Documents	1NonFinalOA0065.pdf	236600 0c55c005668c2b71693871ae352b78009c5116c6	no	6
Warnings:					
Information:					
18	NPL Documents	1NonFinalOA0073.pdf	303829 a6a723e3ac667a3da55f6e3cb49f67261a77bda8	no	8
Warnings:					
Information:					

19	NPL Documents	2FinalOA0015.pdf	292139 ad527a1b0a86de5d988c2194c748c66c065369e9	no	7
Warnings:					
Information:					
20	NPL Documents	2FinalOA0063.pdf	263511 2446c629ae2dd906bd0b9861b51e533e84137e91	no	7
Warnings:					
Information:					
21	NPL Documents	2FOA0016.pdf	257069 7c7fb1bf1686132eb2c2ee6691c4410859627b87	no	7
Warnings:					
Information:					
22	NPL Documents	2NFOA0012.pdf	332065 1d8b7b1031460a352317242875d458835897f69f	no	9
Warnings:					
Information:					
23	NPL Documents	2NFOA0016.pdf	353492 126d54025757372eaf3d0be8302e46a9bef6fd3b	no	10
Warnings:					
Information:					
24	NPL Documents	2NFOA0037.pdf	441997 23c25d7fbe54c7a4050b5b85de419b7051a6b986	no	13
Warnings:					
Information:					
25	NPL Documents	2NOA0012.pdf	476792 88f7e4412687f2f2b615146f665def89a289849a	no	12
Warnings:					
Information:					
26	NPL Documents	2NOA0016.pdf	261219 e5c1f64ccb5409d95d08099de9f67d902a82f729	no	9
Warnings:					
Information:					
27	NPL Documents	2NOA0037.pdf	134374 f178961c33e0503ef5e11c9212f5009a40c08398	no	4
Warnings:					
Information:					

28	NPL Documents	2NonFinalOA0015.pdf	323107 56b716987e27dd46ca5b0389001ca87b6fcf05d7	no	9
Warnings:					
Information:					
29	NPL Documents	2NonFinalOA0065.pdf	340763 96a8385a1e5faa5f2c3423c947fba8a97dc0c462	no	8
Warnings:					
Information:					
30	NPL Documents	2NonFinalOA0073.pdf	428799 97d2e677c0c43b1a8ed09a265cc6b67b5822c8e6	no	11
Warnings:					
Information:					
31	NPL Documents	3NFOA0012.pdf	238086 ca068249588eabbe753fe79517fabfae5556430a	no	6
Warnings:					
Information:					
32	NPL Documents	3NOA0037.pdf	153481 3f0794384d7965215a9e29a921cb89a1bc15366f	no	5
Warnings:					
Information:					
33	NPL Documents	3NonFinalOA0073.pdf	432059 f1d0cff6f09ff3ca021b18811eba4aa8691e08c4	no	10
Warnings:					
Information:					
34	NPL Documents	4NFOA0012.pdf	278018 5719db306528ebec2b9f9d28832dfb2b42ea3131	no	8
Warnings:					
Information:					
35	NPL Documents	4NOApdf0037.pdf	245918 3e81635e443e7c50af72385796adff0615e919b4	no	4
Warnings:					
Information:					
36	NPL Documents	5NFOA0012.pdf	276673 5ff6ce4b17fad949c3d66a2b5f1dfd43af58b281	no	7
Warnings:					
Information:					

37	NPL Documents	5NOA0037.pdf	256957 adf903f072f1875c8fc6a88d49db239669f50 6b9	no	4
Warnings:					
Information:					
38	NPL Documents	1NFOA0042.pdf	286408 6af393892203986735l9a2cc709d52bbb90 75f9b	no	7
Warnings:					
Information:					
39	NPL Documents	1NOA0012.pdf	460543 15719d6b53d2517e10cd744e814aa73bed bd7745	no	9
Warnings:					
Information:					
40	NPL Documents	1NOA0016.pdf	489537 66ee422cb81039180e68e87bf7973aeed11 0638b	no	13
Warnings:					
Information:					
41	NPL Documents	1NOA0037.pdf	306134 ab231a5d73bbda34e9693f4d92017c06911 4c63d	no	6
Warnings:					
Information:					
42	NPL Documents	1NOA0038.pdf	259777 797ddaeb623304528a4d92348af178b3b68 1aa44	no	4
Warnings:					
Information:					
43	NPL Documents	1NOA0039.pdf	309545 38207b9a7789d7b6d60d9723f1533cba93e 8f9fc	no	5
Warnings:					
Information:					
44	NPL Documents	1NOA0065.pdf	339321 a7a2aaadaf5f277e3355417519807fae446fd 0d5	no	7
Warnings:					
Information:					
45	NPL Documents	2FinalOA0044.pdf	267254 1e75f15d18f0b7144aa36fadc447eeac5fde 10b3	no	9
Warnings:					
Information:					

46	NPL Documents	2NOA0065.pdf	300897 b66be01f064494dd688d64b12d429cdb91cde16e	no	7
Warnings:					
Information:					
47	NPL Documents	3NOA0065.pdf	669688 36c0966cd6726ca8b4caf3af0e1519889599b952	no	11
Warnings:					
Information:					
48	NPL Documents	4NOA0065.pdf	249932 0a4f69ed1e6582dc49e7215e13927c119559250a	no	4
Warnings:					
Information:					
49	NPL Documents	5NOA0065.pdf	249890 de3fcfc4c306aa6d3e121ea7ee1ffa950d770b30	no	4
Warnings:					
Information:					
50	NPL Documents	NFOA064.PDF	299991 5c0bdd507ad39c5a25518390b7356cb12e18493c	no	10
Warnings:					
Information:					
51	NPL Documents	Freier.pdf	478992 feed2523b7a389a23e7384771b1003c94f0be1d0	no	59
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
52	NPL Documents	Bequai.pdf	935039 c31352316f6f7f24110e4573adb1a08f9e728a3c	no	6
Warnings:					
Information:					
53	NPL Documents	Chapman.pdf	1713700 39c5c492b168aa3e7de9fca2a4031545bed0e957	no	19
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					

54	NPL Documents	Clark.pdf	967743 84d5d465ebf9b015636fa7bfbf5971c076a8a959	no	4
Warnings:					
Information:					
55	NPL Documents	Davila.pdf	461212 0300df8d7b65f715e893e7e8d5e7985e93b9ed97	no	18
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
56	NPL Documents	depogarytomlinson.pdf	3836799 17defcb699cf68c190c09efa8512cd6c4b47bf31	no	60
Warnings:					
Information:					
57	NPL Documents	Dolev.pdf	17452464 140936b324efe289876400515183 32b3b82f540f	no	15
Warnings:					
Information:					
58	NPL Documents	Eastlake.pdf	1007823 7f990c13c14c9426828dd74c35dd10f320f607b2	no	45
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
59	NPL Documents	Halsall.pdf	2130139 06d0605e6f15e77bee85164e375b3905fc72b1cf	no	49
Warnings:					
Information:					
60	NPL Documents	Glossary.pdf	492648 ab99a978db9beaa32d01031e74a5787d327d2f75	no	27
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
61	Fee Worksheet (PTO-875)	fee-info.pdf	30626 cfe0a73c2ab22cfe32328938984e9bedb25001d8	no	2
Warnings:					

Information:	
Total Files Size (in bytes):	46216011

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	**11/839,987**
Filing Date	**08-16-2007**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Lim, Krisna**
Docket Number	**077580-0066**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1021	4,920,484	04-24-1990	Ranade	
	A1022	4,933,846	06-12-1990	Humphrey et al.	
	A1023	4,988,990	01-29-1991	Warrior	
	A1024	5,164,988	11-17-1992	Matyas	
	A1025	5,276,735	01-04-1994	Boebert et al.	
	A1026	5,329,521	07-12-1994	Walsh et al.	
	A1027	5,341,426	08-23-1994	Barney et al.	
	A1028	5,367,643	11-22-1994	Chang et al.	
	A1029	5,559,883	09-24-1996	Williams	
	A1030	5,561,669	10-01-1996	Lenney et al.	
	A1031	5,588,060	12-24-1996	Aziz	
	A1032	5,625,626	04-29-1997	Umekita	
	A1033	5,654,695	08-05-1997	Olnowich et al.	
	A1034	5,682,480	10-28-1997	Nakagawa	
	A1035	5,689,566	11/18/1997	Nguyen	
	A1036	5,740,375	04-14-1998	Dunne et al.	
	A1037	5,774,660	06-30-1998	Brendel et al.	
	A1038	5,787,172	07-28-1998	Arnold	
	A1039	5,790,548	08-04-1998	Sitaraman et al.	
	A1040	5,796,942	08-18-1998	Esbensen	
	A1041	5,805,801	09-08-1998	Holloway et al.	
	A1042	5,842,040	11-24-1998	Hughes et al.	
	A1043	5,845,091	12-01-1998	Dunne et al.	
	A1044	5,867,650	02-02-1998	Osterman	
	A1045	5,878,231	05-02-1999	Baehr et al.	
	A1046	5,892,903	04-06-1999	Klaus	
	A1047	5,905,859	05-18-1999	Holloway et al.	
	A1048	5,918,018	06/29/1999	Gooderum et al.	
	A1049	5,918,019	06-29-1999	Valencia	
	A1050	5,996,016	11-30-1999	Thalheimer et al.	
	A1051	6,006,259	12-21-1999	Adelman et al.	
	A1052	6,006,272	12-21-1999	Aravamudan et al.	
	A1053	6,016,318	01-18-2000	Tomoike	
	A1054	6,016,512	01-18-2000	Huitema	
	A1055	6,041,342	03-21-2000	Yamaguchi	

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	11/839,987
Filing Date	08-16-2007
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Lim, Krisna
Docket Number	077580-0066

	A1056		6,061,736	05-09-2000	Rochberger et al.	
	A1057		6,092,200	07-18-2000	Muniyappa et al.	
	A1058		6,119,234	09-12-2000	Aziz et al.	
	A1059		6,147,976	11-14-2000	Shand et al.	
	A1060		6,157,957	12-05-2000	Berthaud	
	A1061		6,158,011	12-05-2000	Chen et al.	
	A1062		6,168,409	01-02-2001	Fare	
	A1063		6,175,867	01-16-2001	Taghadoss	
	A1064		6,178,409	01-23-2001	Weber et al.	
	A1065		6,178,505	01-23-2001	Schneider et al.	
	A1066		6,179,102	01-30-2001	Weber et al.	
	A1067		6,222,842	04-24-2001	Sasyan et al.	
	A1068		6,233,618	05-15-2001	Shannon	
	A1069		6,243,360	06-05-2001	Basilico	
	A1070		6,243,749	06-05-2001	Sitaraman et al.	
	A1071		6,243,754	06-05-2001	Guerin et al.	
	A1072		6,256,671	07-03-2001	Strentzsch et al.	
	A1073		6,263,445	07-17-2001	Blumenau	
	A1074		6,286,047	09-04-2001	Ramanathan et al.	
	A1075		6,301,223	10-09-2001	Hrastar et al.	
	A1076		6,308,213	10/23/2001	Valencia	
	A1077		6,308,274	10-23-2001	Swift	
	A1078		6,311,207	10-30-2001	Mighdoll et al.	
	A1079		6,324,161	11-27-2001	Kirch	
	A1080		6,330,562	12-11-2001	Boden et al.	
	A1081		6,332,158	12-18-2001	Risley et al.	
	A1082		6,353,614	03-05-2002	Borella et al.	
	A1083		6,425,003	07-23-2002	Herzog et al.	
	A1084		6,430,155	08-06-2002	Davie et al.	
	A1085		6,430,610	08-06-2002	Carter	
	A1086		6,487,598	11-26-2002	Valencia	
	A1087		6,505,232	01-07-2003	Mighdoll et al.	
	A1088		6,510,154	01-21-2003	Mayes et al.	
	A1089		6,549,516	04-15-2003	Albert et al.	
	A1090		6,571,296	05-27-2002	Dillon	
	A1091		6,571,338	05-27-2003	Shaio et al.	
	A1092		6,581,166	07-17-2003	Hirst et al.	
	A1093		6,606,708	08-12-2003	Devine et al.	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

	A1094	6,618,761	09-09-2003	Munger et al.	
	A1095	6,671,702	12-30-2003	Kruglikov et al.	
	A1096	6,687,551	02-03-2004	Steindl	
	A1097	6,714,970	03-30-2004	Fiveash et al.	
	A1098	6,717,949	04-06-2004	Boden et al.	
	A1099	6,751,738	06-15-2004	Wesinger, Jr. et al.	
	A1100	6,760,766	07-06-2004	Sahlqvist	
	A1101	6,826,616	11-30-2004	Larson et al.	
	A1102	6,839,759	01-04-2005	Larson et al.	
	A1103	7,010,604	03-07-2006	Munger et al.	
	A1104	7,133,930	11-07-2006	Munger et al.	
	A1105	7,188,180	03-06-2007	Larson et al.	
	A1106	7,197,563	03-27-2007	Sheymov et al.	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B1	US2002/0004898	01-10-2002	Droge	
	B2	US2003/0196122	10-16-2003	Wesinger, Jr., et al.	
	B3	US2005/0055306	03-10-2005	Miller et al.	
	B4	US2006/0059337	03-16-2006	Polyhonen et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 -Number 4 -Kind Codes5 *(if known)*	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	C1010	DE19924575	12-02-1999	Provino et al.			
	C1011	EP0858189	08-12-1998	Maciel et al.			
	C1012	EP836306	04-15-1998	Hewlett Packard Co.			
	C1013	WO0150688	07-12-2001	Kriens			
	C1014	WO9855930	12-10-1998	Tang			
	C1015	WO9859470	12-30-1998	Kanter et al.			
	C1016	WO9938081	07-29-1999	Paulsen et al.			
	C1017	WO9948303	09-23-1999	Cox et al.			

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1254	Alan 0. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/ draft302.txt on Feb. 4, 2002, 56 pages.	
	D1255	August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.	
	D1256	D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-375.	
	D1257	D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.	
	D1258	Davila J et al, "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Work-shop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-666.	
	D1259	Deposition Transcript for Gary Tomlinson dated February 27, 2009.	
	D1260	Dolev, Shlomi and Ostrovsky, Rafil, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.	
	D1261	Donald E. Eastlake, 3rd, "Domain Name System Security Extensions", INTERNET DRAFT, Apr. 1998, pp. 1-51.	
	D1262	F. Halsall, "Data Communications, Computer Networks and Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.	
	D1263	Final Office Action dated April 11,2005 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016).	
	D1264	Final Office Action dated April 8, 2010 from corresponding US Application Number 11/679,416 (Our Ref. No.077580-0015).	
	D1265	Final Office Action dated December 7, 2005 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037).	
	D1266	Final Office Action dated February 11, 2004 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016).	
	D1267	Final Office Action dated February 9, 2010 from corresponding US Application Number 11/301,022 (Our Ref. No.077580-0044).	
	D1268	Final Office Action dated October 21, 2010 from corresponding US Application Number 11/840,560 (Our Ref. No.077580-0063).	
	D1269	Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/ doc/glossary.html on Feb. 21, 2002, 25 pages.	
	D1270	J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan _trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

	D1271	James E. Bellaire, "New Statement of Rules-Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page. (Due to difficulty finding a hard copy of this reference, a copy of this reference is not included herewith. This reference, however was first submitted to the Patent Office in an IDS in application No. 11/679,416 on 11/13/2007 as ref. No. C12. The office is requested to see this reference at that location).	
	D1272	Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.	
	D1273	Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606, 1 page.	
	D1274	Linux FreeS/WAN Index File, printed from http://liberty.freewan.org/freeswan_trees/freeswan-1.3/doc/ on Feb. 21, 2002, 3 Pages. (Due to difficulty finding a hard copy of this reference, a copy of this reference is not included herewith. This reference, however was first submitted to the Patent Office in an IDS in application No. 11/679,416 on 11/13/2007 as ref. No. C15. The office is requested to see this reference at that location).	
	D1275	Non-Final Office Action dated December 14, 2010 from corresponding US Application Number 11/839,937 (Our Ref. No. 077580-0064)	
	D1276	Non-Final Office Action dated December 7, 2010 from corresponding US Application Number 11/679,416 (Our Ref. No. 077580-0015)	
	D1277	Notice of Allowance dated January 11, 2008 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D1278	Non-Final Office Action dated July 1, 2010 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065).	
	D1279	Non-Final Office Action dated July 14, 2010 from corresponding US Application Number 11/840,508 (Our Ref. No.077580-0057).	
	D1280	Non-Final Office Action dated June 15, 2007 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D1281	Non-Final Office Action dated June 16, 2003 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016).	
	D1282	Non-Final Office Action dated June 24, 2004 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D1283	Non-Final Office Action dated June 3, 2005 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037.	
	D1284	Non-Final Office Action dated June 7, 2010 from corresponding US Application Number 11/924,460 (Our Ref. No.077580-0073).	
	D1285	Non-Final Office Action dated June 8, 2009 from corresponding US Application Number 11/679,416 (Our Ref. No.077580-0015).	
	D1286	Non-Final Office Action dated June 9, 2010 from corresponding US Application Number 11/924,460 (Our Ref. No.077580-0073).	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

	D1287	Non-Final Office Action dated March 1, 2004 from corresponding US Application Number 10/401,888 (Our Ref. No. 077580-0038)	
	D1288	Non-Final Office Action dated March 19, 2010 from corresponding US Application Number 11/840,560 (Our Ref. No.077580-0063).	
	D1289	Non-Final Office Action dated March 21, 2007 from corresponding US Application Number 10/714,849 (Our Ref. No. 077580-0042)	
	D1290	Non-Final Office Action dated March 28, 2006 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D1291	Non-Final Office Action dated March 5, 2009 from corresponding US Application Number 11/301,022 (Our Ref. No.077580-0044).	
	D1292	Non-Final Office Action dated May 19, 2006 from corresponding US Application Number 10/702,486 (Our Ref. No.077580-0039).	
	D1293	Non-Final Office Action dated May 4, 2004 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016).	
	D1294	Non-Final Office Action dated October 18, 2005 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D1295	Non-Final Office Action dated October 21, 2004 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037).	
	D1296	Non-Final Office Action dated October 30, 2006 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D1297	Non-Final Office Action dated September 17, 2008 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065).	
	D1298	Non-Final Office Action dated September 2, 2009 from corresponding US Application Number 11/924,460 (Our Ref. No.077580-0073).	
	D1299	Notice of Allowance dated April 18, 2006 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D1300	Notice of Allowance dated April 3, 2009 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	
	D1301	Notice of Allowance dated April 5, 2006 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D1302	Notice of Allowance dated August 10, 2005 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016)	
	D1303	Notice of Allowance dated August 16, 2004 from corresponding US Application Number 10/702,580 (Our Ref. No. 077580-0041)	
	D1304	Notice of Allowance dated August 17, 2004 from corresponding US Application Number 10/702,522 (Our Ref. No. 077580-0040)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

	D1305	Notice of Allowance dated December 5, 2005 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016)	
	D1306	Notice of Allowance dated February 16, 2006 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D1307	Notice of Allowance dated January 13, 2010 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	
	D1308	Notice of Allowance dated January 28, 2010 from corresponding US Application Number 11/840,508 (Our Ref. No.077580-0057)	
	D1309	Notice of Allowance dated January 4, 2011 from corresponding US Application Number 11/301,022 (Our Ref. No. 077580-0044)	
	D1310	Notice of Allowance dated July 1, 2008 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D1311	Notice of Allowance dated July 21, 2004 from corresponding US Application Number 10/401,888 (Our Ref. No. 077580-0038)	
	D1312	Notice of Allowance dated March 17, 2006 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D1313	Notice of Allowance dated May 27, 2009 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	
	D1314	Notice of Allowance dated May 9, 2006 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D1315	Notice of Allowance dated November 19, 2009 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	
	D1316	Notice of Allowance dated November 21, 2006 from corresponding US Application Number 10/702,486 (Our Ref. No.077580-0039)	
	D1317	Notice of Allowance dated October 29, 2007 from corresponding US Application Number 10/714,849 (Our Ref. No. 077580-0042)	
	D1318	Notice of Allowance dated September 16, 2009 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	
	D1319	P. Srisuresh et al., "DNS extensions to Network address Translators (DNS_ALG)", Internet Draft, Jul. 1998, pp. 1-27.	
	D1320	PCT International Search Report for related PCT Application No.: PCT/US01/13261, 8 pages (Our Ref. No. 077580-0032).	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

	D1321	PCT International Search Report for related PCT Application No.: PCT/US99/25323, 3 pages (Our Ref. No. 077580-0062).	
	D1322	PCT International Search Report for related PCT Application No.: PCT/US99/25325, 3 pages (Our Ref. No. 077580-0061).	
	D1323	Reiter, Michael K. and Rubin, Aviel D. (AT&T Labs-Research), "Crowds: Anonymity for Web Transactions", pp. 1-23.	
	D1324	RFC 2401 (dated Nov. 1998) Security Architecture for the Internet Protocol (RTP).	
	D1325	RFC 2543-SIP (dated March 1999): Session Initiation Protocol (SIP or SIPS).	
	D1326	Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages. (Due to difficulty finding a hard copy of this reference, a copy of this reference is not included herewith. This reference, however was first submitted to the Patent Office in an IDS in application No. 11/679,416 on 11/13/2007 as ref. No. C20. The office is requested to see this reference at that location).	
	D1327	Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.	
	D1328	Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.	
	D1329	Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.	
	D1330	Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.	
	D1331	Search Report, IPER (dated Jan. 14, 2003), International Application No. PCT/US01/13260.	
	D1332	Search Report, IPER (dated Nov. 13, 2002), International Application No. PCT/US01/04340.	
	D1333	Shankar, A.U. "A verified sliding window protocol with variable flow control". Proceedings of ACM SIGCOMM conferece on Communications architectures & protocols. pp. 84-91, ACM Press, NY,NY 1986.	
	D1334	Shree Murthy et al., "Congestion-Oriented Shortest Multi-path Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.	
	D1335	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 9:00 AM.	
	D1336	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 1:00 PM.	
	D1337	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 9:00 AM.	
	D1338	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 1:30 PM.	
	D1339	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 9:00 AM.	
	D1340	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 1:15 PM.	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

	D1341	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 9:00 AM.	
	D1342	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 12:35 PM.	
	D1343	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 8:45 AM.	
	D1344	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 1:30 PM.	
	D1345	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 9:00 AM.	
	D1346	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 1:30 PM.	
	D1347	W. Stallings, "Cryptography And Network Security", 2nd, Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[X] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Toby H. Kusmer

Date: 2/9/11

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 27365439-1.077580.0066

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2001 (15.11.2001)

PCT

(10) International Publication Number
WO 01/086911 A3

(51) International Patent Classification[7]: H04L 29/06, 29/12

(21) International Application Number: PCT/US01/13261

(22) International Filing Date: 25 April 2001 (25.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/558,209 26 April 2000 (26.04.2000) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier applications:

US	09/558,209 (CON)
Filed on	26 April 2000 (26.04.2000)
US	09/429,643 (CON)
Filed on	29 October 1999 (29.10.1999)
US	09/504,783 (CON)
Filed on	15 February 2000 (15.02.2000)
US	60/137,704 (CON)
Filed on	7 June 1999 (07.06.1999)
US	60/106,261 (CON)
Filed on	30 October 1998 (30.10.1998)

(71) Applicant *(for all designated States except US)*: **SCIENCE APPLICATIONS INTERNATIONAL CORPORATION** [US/US]; 10260 Campus Point Drive, MS#F3, San Diego, CA 92121 (US).

(71) Applicants and
(72) Inventors: **LARSON, Victor** [US/US]; 12026 Lisa Marie Court, Fairfax, VA 22033 (US). **SHORT, Robert, Durham, III** [US/US]; 38710 Goose Creek Lane, Leesburg, VA 20175 (US). **MUNGER, Edmund, Colby** [US/US]; 1101 Opaca Court, Crownsville, MD 21032 (US). **SCHMIDT, Douglas, Charles** [US/US]; 230 Oak Court, Severna Park, MD 21146 (US). **WILLIAMSON, Michael** [US/US]; 26203 Ocala Circle, South Riding, VA 20152 (US).

(74) Agents: **CURTIN, Joseph, P.** et al.; Banner & Witcoff, Ltd., 1001 G Street, N.W., Eleventh Floor, Washington, DC 20001-4597 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
6 February 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/086911 A3

(54) Title: PROTOCOL FOR SECURE COMMUNICATIONS

(57) Abstract: A technique is disclosed for establishing a secure communication link between a first computer and a second computer over a computer network. Initially, a secure communication mode of communication is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. The secure communication link is a virtual private network communication link over the computer network in which one or more data values that vary according to a pseudo-random sequence are inserted into each data packet.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/13261

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L29/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ, WPI Data, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 838 930 A (DIGITAL EQUIPMENT CORP) 29 April 1998 (1998-04-29)	1,8,16, 23,53, 54, 56-58, 63-65, 67-69, 74-76, 78-80, 85-87, 89-91, 96-98, 100,101, 106-108, 110,111, 116
Y	abstract	2,4-7, 9-14,17, 18, 20-22,
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 September 2002	07.10.2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bertolissi, E

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
		24-29, 55, 59-62, 66, 70-73, 77, 81-84, 88, 92-95, 99, 102-105, 109, 112-115
	column 3, line 30 -column 4, line 14 column 16, line 12 -column 17, line 14 column 22, line 56 -column 23, line 20 figures 3,4,9,11-13,21,22 ---	
X	GB 2 317 792 A (SECURE COMPUTING CORP) 1 April 1998 (1998-04-01)	1,4,8, 14,16, 18,23, 29, 53-58, 63-69, 74-80, 85-91, 96-101, 106-111, 116
Y	abstract	15,30, 31,34, 36,41, 42,45, 47,52
	page 2, line 3 - line 25 page 3, line 1 - line 10 page 8, line 18 - line 24 page 10, line 20 -page 12, line 2 page 12, line 26 - line 31 page 13, line 16 - line 29 figures 1-4 ---	
Y	EP 0 814 589 A (AT & T CORP) 29 December 1997 (1997-12-29) page 1, line 45 -page 2, line 2 page 5, line 8 - line 14 ---	2,17
X	US 5 588 060 A (AZIZ ASHAR) 24 December 1996 (1996-12-24)	1,3,16, 19
Y	abstract	59,70, 81,92, 102,112
	column 4, line 38 - line 46 column 6, line 50 - line 67 figure 2 --- -/--	

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/13261

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 689 566 A (NGUYEN MINHTAM C) 18 November 1997 (1997-11-18) abstract column 9, line 10 -column 10, line 4 ---	4,9,10, 14,18, 24,25, 29,55, 66,77, 88,99, 109
Y	WO 98 27783 A (NORTHERN TELECOM LTD ;HOLMES KIM (US); HUI MARGARET (US); TELLO AN) 25 June 1998 (1998-06-25) abstract figure 3 ---	11,26
Y	LAURIE WELLS (LANCASTERB1B@EMAIL.MSN.COM): "Subject: Security Icon" USENET NEWSGROUP, 'Online! 19 October 1998 (1998-10-19), XP002200606 microsoft.public.inetexplorer.ie4.security Retrieved from the Internet: <URL:http://groups.google.com/> 'retrieved on 2002-05-30! the whole document ---	12,13, 27,28
A	STALLINGS W: "CRYPTOGRAPHY AND NETWORK SECURITY, PRINCIPLES AND PRACTICE, 2ND EDITION" CRYPTOGRAPHY AND NETWORK SECURITY, XX, XX, 8 June 1998 (1998-06-08), pages 399-440, XP002167283 13.4 Encapsulating security payload 13.5 Combining security associations ---	53-59, 63-70, 74-81, 85-92, 96-102, 106-112, 116
L	WILLIAM STALLINGS (WS@SHORE.NET): "Subject: new cryptography and network security book" USENET NEWSGROUP, 'Online! 8 June 1998 (1998-06-08), XP002200607 comp.security.misc Retrieved from the Internet: <URL:http://groups.google.com/> 'retrieved on 2002-05-30! Proof of publication date of XP002167283 ---	

-/--

INTERNATIONAL SEARCH REPORT

national Application No
PCT/US 01/13261

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 98 55930 A (KONINKL PHILIPS ELECTRONICS NV ;PHILIPS SVENSKA AB (SE)) 10 December 1998 (1998-12-10) abstract page 16, line 21 -page 18, line 20; figures 2,3 ---	5,7,20, 22,60, 62,71, 73,82, 84,93, 95,103, 105,113, 115
Y	HALSALL F.: " DATA COMMUNICATIONS, COMPUTER NETWORKS AND OPEN SYSTEMS" 1996 , ADDISON-WESLEY XP002214366	6,21,61, 72,83, 94,104, 114
A	page 198 -page 203 Sliding window 4.3.4 Sequence numbers ---	38,49
Y	EASTLAKE D E: "Domain Name System Security Extensions" INTERNET DRAFT, April 1998 (1998-04), XP002199931 abstract 1. Overview of the Contents 2.3 Data origin authentication and integrity 2.4 DNS transaction and request authentication ---	15,30, 31,34, 36,41, 42,45, 47,52
A	CHAPMAN D B ET AL: "Building Internet Firewalls" BUILDING INTERNET FIREWALLS, SEBASTOPOL, CA: O'REILLY, US, 1995, pages 278-296,351-375, XP002199932 ISBN: 1-56592-124-0 page 286 -page 296 -----	31-52

International application No.
PCT/US 01/13261

INTERNATIONAL SEARCH REPORT

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet (1)) (July 1998)

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-4 8-14 16-19 23-29 53-59 63-70 74-81 85-92 96-102 106-112 116

   A method and computer readable medium for loading a secure communication software module

2. Claims: 5-7 (as dependent from 1) 20-22 (as dependent from 16) 60-62 (as dependent from 53) 71-73 (as dependent from 64) 82-84 (as dependent from 75) 93-95 (as dependent from 86) 103-105 (as dependent from 97) 113-115 (as dependent from 107)

   A method and computer readable medium based on a computer address hopping regime

3. Claims: 15 (as dependent from 1), 30 (as dependent from 16), 31-52

   A method and computer readable medium for sending a query for a secure network addess to a secure domain name server

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 01/13261

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0838930	A	29-04-1998	US	6101543 A	08-08-2000
			EP	0838930 A2	29-04-1998
			JP	10178450 A	30-06-1998
GB 2317792	A	01-04-1998	US	5983350 A	09-11-1999
			US	5950195 A	07-09-1999
			DE	19741239 A1	07-05-1998
			DE	19741246 A1	19-03-1998
			GB	2317539 A ,B	25-03-1998
EP 0814589	A	29-12-1997	US	6058250 A	02-05-2000
			CA	2204058 A1	19-12-1997
			EP	0814589 A2	29-12-1997
US 5588060	A	24-12-1996	EP	0693836 A1	24-01-1996
			JP	8008895 A	12-01-1996
			US	5668877 A	16-09-1997
			US	5633933 A	27-05-1997
			US	6091820 A	18-07-2000
			US	6026167 A	15-02-2000
US 5689566	A	18-11-1997	US	5638448 A	10-06-1997
WO 9827783	A	25-06-1998	US	6032118 A	29-02-2000
			AU	727878 B2	04-01-2001
			AU	5131198 A	15-07-1998
			DE	19782193 D2	25-11-1999
			EP	1008275 A1	14-06-2000
			GB	2336511 A ,B	20-10-1999
			WO	9827783 A1	25-06-1998
			JP	2002514362 T	14-05-2002
			SE	9902261 A	16-06-1999
WO 9855930	A	10-12-1998	EP	0914635 A1	12-05-1999
			WO	9855930 A1	10-12-1998
			JP	2000516734 T	12-12-2000
			US	6185682 B1	06-02-2001

Form PCT/ISA/210 (patent family annex) (July 1992)

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06

A3

(11) International Publication Number: WO 00/27090

(43) International Publication Date: 11 May 2000 (11.05.00)

(21) International Application Number: PCT/US99/25323

(22) International Filing Date: 29 October 1999 (29.10.99)

(30) Priority Data:

60/106,261	30 October 1998 (30.10.98)	US
60/137,704	7 June 1999 (07.06.99)	US

(71) Applicant (*for all designated States except US*): SCIENCE APPLICATIONS INTERNATIONAL CORPORATION [US/US]; 10260 Campus Point Drive, San Diego, CA 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): MUNGER, Edmund, C. [US/US]; 1101 Opaca Court, Crownsville, MD 21032 (US). SABIO, Vincent, J. [US/US]; 7489 Setting Sun Way, Columbia, MD 21046 (US). SHORT, Robert, Dunham, III [US/US]; 38710 Goose Creek Lane, Leesburg, VA 20175 (US). GLIGOR, Virgil, D. [US/US]; 6009 Brookside Drive, Chevy Chase, MD 20815 (US). SCHMIDT, Douglas, Charles [US/US]; 230 Oak Court, Severna Park, MD 21146 (US).

(74) Agents: WRIGHT, Bradley, C. et al.; Banner & Witcoff, Ltd., Eleventh floor, 1001 G Street, N.W., Washington, DC 20001–4597 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

(88) Date of publication of the international search report: 12 October 2000 (12.10.00)

(54) Title: NETWORK PROTOCOL FOR SECURE COMMUNICATIONS

(57) Abstract

A plurality of computer nodes communicates using seemingly random IP source and destination addresses and (optionally) a seemingly random discriminator field. Data packets matching criteria defined by a moving window of valid addresses are accepted for further processing, while those that do not meet the criteria are rejected. In addition to "hopping" of IP addresses and discriminator fields, hardware addresses such as Media Access Control addresses can be hopped. The hopped addresses are generated by random number generators having non–repeating sequence lengths that are easily determined a–priori, which can quickly jump ahead in sequence by an arbitrary number of random steps and which have the property that future random numbers are difficult to guess without knowing the random number generator's parameters. Synchronisation techniques can be used to re–establish synchronization between sending and receiving nodes. These techniques include a self–synchronization technique in which a sync field is transmitted as part of each packet, and a "checkpoint" scheme by which transmitting and receiving nodes can advance to a known point in their hopping schemes. A fast–packet reject technique based on the use of presence vectors is also described.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERNATIONAL SEARCH REPORT

Int· tional Application No
PCT/US 99/25323

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FASBENDER A ET AL: "VARIABLE AND SCALABLE SECURITY: PROTECTION OF LOCATION INFORMATION IN MOBILE IP" IEEE VEHICULAR TECHNOLOGY CONFERENCE,US,NEW YORK, IEEE, vol. CONF. 46, 1996, pages 963-967, XP000593113 ISBN: 0-7803-3158-3 the whole document -----	1-63

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 July 2000	27/07/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Canosa Aresté, C

3

Form PCT/ISA/210 (second sheet) (July 1992)

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06

A3

(11) International Publication Number: WO 00/27086

(43) International Publication Date: 11 May 2000 (11.05.00)

(21) International Application Number: PCT/US99/25325

(22) International Filing Date: 29 October 1999 (29.10.99)

(30) Priority Data:

60/106,261	30 October 1998 (30.10.98)	US
60/137,704	7 June 1999 (07.06.99)	US

(63) Related by Continuation (CON) or Continuation-in-Part (CIP) to Earlier Applications

US	60/106,261 (CON)
Filed on	30 October 1998 (30.10.98)
US	60/137,704 (CON)
Filed on	7 June 1999 (07.06.99)

(71) Applicant *(for all designated States except US)*: SCIENCE APPLICATIONS INTERNATIONAL CORPORATION [US/US]; 10260 Campus Point Drive, San Diego, CA 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: MUNGER, Edmund, C. [US/US]; 1101 Opaca Court, Crownsville, MD 21032 (US). SABIO, Vincent, J. [US/US]; 7489 Setting Sun Way, Columbia, MD 21046 (US). SHORT, Robert, Dunham, III [US/US]; 38710 Goose Creek Lane, Leesburg, VA 20175 (US). GLIGOR, Virgil, D. [US/US]; 6009 Brookside Drive, Chevy Chase, MD 20815 (US). SCHMIDT, Douglas, Charles [US/US]; 230 Oak Court, Severna Park, MD 21146 (US).

(74) Agents: WRIGHT, Bradley, C. et al.; Banner & Witcoff, Ltd., Eleventh floor, 1001 G Street, N.W., Washington, DC 20001-4597 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

(88) Date of publication of the international search report: 5 October 2000 (05.10.00)

(54) Title: NETWORK PROTOCOL FOR SECURE COMMUNICATIONS

(57) Abstract

A plurality of computer nodes communicates using seemingly random IP source and destination addresses and (optionally) a seemingly random discriminator field. Data packets matching criteria defined by a moving window of valid addresses are accepted for further processing, while those that do not meet the criteria are rejected. In addition to "hopping" of IP addresses and discriminator fields, hardware addresses such as Media Access Control addresses can be hopped. The hopped addresses are generated by random number generators having non-repeating sequence lengths that are easily determined a-priori, which can quickly jump ahead in sequence by an arbitrary number of random steps and which have the property that future random numbers are difficult to guess without knowing the random number generator's parameters. Synchronization techniques can be used to re-establish synchronization between sending and receiving nodes. These techniques include a self-synchronization technique in which a sync field is transmitted as part of each packet, and a "checkpoint" scheme by which transmitting and receiving nodes can advance to a known point in their hopping schemes. A fast-packet reject technique based on the use of presence vectors is also described. A distributed transmission path embodiment incorporates randomly selected physical transmission paths.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERNATIONAL SEARCH REPORT

Int ·tional Application No
PCT/US 99/25325

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FASBENDER A ET AL: "VARIABLE AND SCALABLE SECURITY: PROTECTION OF LOCATION INFORMATION IN MOBILE IP" IEEE VEHICULAR TECHNOLOGY CONFERENCE,US,NEW YORK, IEEE, vol. CONF. 46, 1996, pages 963-967, XP000593113 ISBN: 0-7803-3158-3 the whole document	1-67

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 July 2000	27/07/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Canosa Aresté, C

1

Form PCT/ISA/210 (second sheet) (July 1992)

REC'D 20 NOV 2002
WIPO PCT

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

(Rationalised Report according to the Notice of the President of the EPO published in the OJ11/2001)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
00479.00029		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US 01/ 04340	12/02/2001	15/02/2000
International Patent Classification (IPC) or national classification and IPC		
H04L12/56		
Applicant		
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 2 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consists of a total of ______ sheets.

3. This report contains indications relating to the following items:

   I ☒ Basis of the report

   II ☐ Priority

   III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

   IV ☒ Lack of unity of invention

   V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

   VI ☐ Certain documents cited

   VII ☐ Certain defects in the international application

   VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
20/08/2001	13/11/2002
Name and mailing address of the IPEA/ European Patent Office D-80298 Munich Tel. (+49-89) 2399-0, Tx: 523656 epmu d Fax: (+49-89) 2399-4465	Authorized officer HEY S A Tel. (+49-89) 2399 2828

EUROPÄISCHES PATENTAMT · EUROPEAN PATENT OFFICE · OFFICE EUROPÉEN DES BREVETS

Form PCT/IPEA/409 (cover sheet) P20476 (October 2002)

I. Basis of the report

The basis of this international preliminary examination is the application as originally filed.

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

If all the additional search fees, which the applicant has been invited to pay, have not been paid, then all the inventions or groups of inventions corresponding to the unpaid fees will not have been searched. This means that the question of whether the claimed invention appears to be novel, to involve an inventive step, or to be industrially applicable has not been the subject of the international preliminary examination in respect of the claims corresponding to these inventions or groups of inventions (Article 17(3)(a) and Rule 66.1(e) PCT; see also international search report).

IV. Lack of unity of invention

The objection as to lack of unity raised in the international search report is maintained. The reasons for the objection are the same as those indicated in the international search report.

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability

To the extent that the international preliminary examination has been carried out (see item III above), the following is pointed out:

In light of the documents cited in the international search report, it is considered that the invention as defined in at least some of the claims, which have been the subject of an international search report, does not appear to meet the criteria mentioned in Article 33(1) PCT, i.e. does not appear to be novel and/or to involve an inventive step (see international search report, in particular the documents cited X and/or Y and corresponding claim references).

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 December 2001 (06.12.2001)

PCT

(10) International Publication Number
WO 01/092997 A3

(51) International Patent Classification[7]: H04L 29/12, 29/06, G06F 17/60

(21) International Application Number: PCT/US01/13260

(22) International Filing Date: 25 April 2001 (25.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/558,210 26 April 2000 (26.04.2000) US

(71) Applicant *(for all designated States except US)*: **SCIENCE APPLICATIONS INTERNATIONAL CORPORATION** [US/US]; 10260 Campus Point Drive, MS #F3, San Diego, CA 92121 (US).

(71) Applicants and
(72) Inventors: **LARSON, Victor** [US/US]; 12026 Lisa Marie Court, Fairfax, VA 22033 (US). **SHORT, Robert, Durham, III** [US/US]; 38710 Goose Creek Lane, Leesburg, VA 20175 (US). **MUNGER, Edmund, Colby** [US/US]; 1101 Opaca Court, Crownsville, MD 21032 (US). **SCHMIDT, Douglas, Charles** [US/US]; 230 Oak Court, Severna Park, MD 21146 (US). **WILLIAMSON, Michael** [US/US]; 26203 Ocala Circle, South Riding, VA 20152 (US).

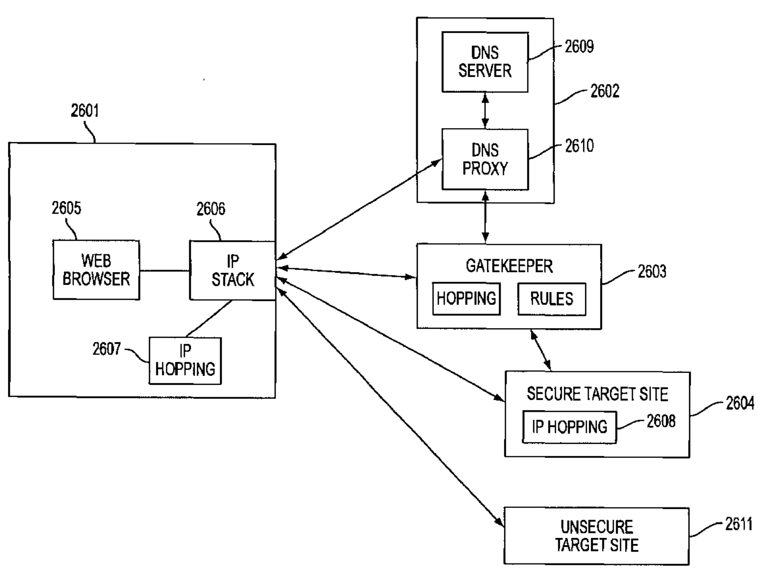
(74) Agents: **CURTIN, Joseph, P.** et al.; Banner & Witcoff, Ltd., 1001 G Street, N.W., Eleventh Floor, Washington, DC 20001-4597 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: SECURE DOMAIN NAME SERVICE



(57) Abstract: A secure domain name service for a computer network is disclosed that includes a portal connected to a computer network, such as the Internet, and a domain name database connected to the computer network through the portal. The portal authenticates a query for a secure computer network address, and the domain name database stores secure computer network addresses for the computer network. Each secure computer network address is based on a non-standard top-level domain name, such as .scom, .sorg, .snet, .snet, .sedu, .smil and .sint.

WO 01/092997 A3

IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report: 17 October 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/13260

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/12 H04L29/06 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DONALD E. EASTLAKE 3RD: "<draft-ietf-dnssec-secext2-05.txt> Domain Name System Security Extensions" INTERNET DRAFT, 'Online! April 1998 (1998-04), XP002199931 Retrieved from the Internet: <URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-dnssec-secext2-05.txt> 'retrieved on 2002-05-23! 1. Overview of the contents 2.3 Data origin authemtication and integrity 2.4 DNS transaction and request authentication --- -/--	1,4-6

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 August 2002	23.08.2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bertolissi, E

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	CHAPMAN D.B.; ZWICKY E.D.: " Building Internet Firewalls" O'REILLY, November 1995 (1995-11), XP002199932 pag 278-296 pag 351-375 ---	1,4-6
P,X	DE 199 24 575 A (SUN MICROSYSTEMS INC) 2 December 1999 (1999-12-02) abstract column 2, line 48 -column 3, line 6 ---	1,4,5,7
A	P. SRISURESH, G. TSIRTSIS, P. AKKIRAJU, A. HEFFERNAN: "<draft-ietf-nat-dns-alg-00.txt> DNS extensions to Network Address Translators (DNS_ALG)" INTERNET DRAFT, 'Online! July 1998 (1998-07), XP002199933 Retrieved from the Internet: <URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-nat-dns-alg-00.txt> 'retrieved on 2002-05-23! 1. Introduction 2. Requirement for DNS extensions fig 3 5.3 Incoming name lookup queries 8. Security considerations ---	1-12
A	EP 0 838 930 A (DIGITAL EQUIPMENT CORP) 29 April 1998 (1998-04-29) abstract column 9, line 11 -column 10, line 34 ---	1-12
X	JAMES E. BELLAIRE: "Subject: New Statement of Rules - Naming Internet Domains " INTERNET NEWSGROUP, 'Online! 30 July 1995 (1995-07-30), XP002209580 comp.dcom.telecom Retrieved from the Internet: <URL:http://groups.google.com/> 'retrieved on 2002-08-12! page 1, paragraph 8 page 2, paragraph 4 ---	13,15
A	CLARK D: "US CALLS FOR PRIVATE DOMAIN-NAME SYSTEM" COMPUTER, IEEE COMPUTER SOCIETY, LONG BEACH., CA, US, US, vol. 31, no. 8, 1 August 1998 (1998-08-01), pages 22-25, XP000780513 ISSN: 0018-9162 page 22 --- -/--	13-16

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	BEQUAI A: "Balancing Legal Concerns Over Crime and Security in Cyberspace" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 17, no. 4, 1998, pages 293-298, XP004129224 ISSN: 0167-4048 pag 296-297 Lanham Act ---	13-16
A	RICH WINKEL : "CAQ: NETWORKING WITH SPOOKS: THE NET & THE CONTROL OF INFORMATION " INTERNMET NEWSGROUP, 'Online! 21 June 1997 (1997-06-21), XP002209581 misc.activism.progressive Retrieved from the Internet: <URL:http://groups.google.com/> 'retrieved on 2002-08-12! the whole document -----	13-16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 01/13260

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [ ] Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. [ ] Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. [X] As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest.

[X] No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-12

   A portal for authenticating a query for a secure computer network address

2. Claims: 13-16

   A method and a computer readable storage medium for registering a secure domain name

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 01/13260

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
DE 19924575	A	02-12-1999	DE	19924575	A1	02-12-1999
			FR	2782873	A1	03-03-2000
			GB	2340702	A ,B	23-02-2000
			JP	2000049867	A	18-02-2000
EP 0838930	A	29-04-1998	US	6101543	A	08-08-2000
			EP	0838930	A2	29-04-1998
			JP	10178450	A	30-06-1998

PATENT COOPERATION TREATY

REC'D 16 JAN 2003
WIPO PCT

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 00479.00028	**FOR FURTHER ACTION** See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/US01/13260	International filing date *(day/month/year)* 25/04/2001	Priority date *(day/month/year)* 26/04/2000
International Patent Classification (IPC) or national classification and IPC H04L29/12		
Applicant SCIENCE APPLICATIONS INTERNATIONAL CORP. et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☒ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
12/11/2001	14.01.2003
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Pajatakis, E Telephone No. +49 89 2399 8898

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/US01/13260

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)):*

Description, pages:

1-92 as originally filed

Claims, No.:

1-15 as originally filed

Drawings, sheets:

1/40-40/40 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:

☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

   (Any replacement sheet containing such amendments must be referred to under Item 1 and annexed to this report.)

6. Additional observations, if necessary:

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:

   ☐ the entire international application.

   ☒ claims Nos. 1-12.

because:

   ☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (*specify*):

   ☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 1-12 are so unclear that no meaningful opinion could be formed (*specify*):
   see separate sheet

   ☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

   ☐ no international search report has been established for the said claims Nos. . .

2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:

   ☐ the written form has not been furnished or does not comply with the standard.

   ☐ the computer readable form has not been furnished or does not comply with the standard.

IV. Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees the applicant has:

   ☐ restricted the claims.

☒ paid additional fees.

☐ paid additional fees under protest.

☐ neither restricted nor paid additional fees.

2. ☐ This Authority found that the requirement of unity of invention is not complied and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

☐ complied with.

☒ not complied with for the following reasons:
see separate sheet

4. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this report:

☒ all parts.

☐ the parts relating to claims Nos. .

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	13-15
	No:	Claims	
Inventive step (IS)	Yes:	Claims	13-15
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	13-15
	No:	Claims	

2. Citations and explanations
see separate sheet

Re Item III

Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. Claims 1-8 are seeking protection for a domain name service. A domain service is the result of executing a method or using an apparatus adapted to retrieve network addresses. Thus, it is not clear whether protection is sought for a method or an apparatus, see also Guidelines III-4.1.

1.1 Claims 9-12 are seeking protection for a method according to Claim 7. However, Claim 7 does not relate to a method.

1.2 The relative term "non-standard" in Claim 2 casts doubt on the scope of protection, see also Guidelines III-4.5.

1.3 An antecedent definition is missing for "the secure communication link" in Claim 8.

1.4 The wording of Claims 9-12 is a statement of the result to be achieved, see also Guidelines III-4.7.

Re Item IV

Lack of unity of invention

1. The application does not meet the requirement of unity, Rule 13.1.

1.1 Independent Claim 1 is directed to resolving queries for a secure network address. This is done by a portal connected to the network, the portal authenticating a query for a secure network address, and by a domain name database connected to the network through the portal, the database storing secure network addresses.

On the other hand independent Claims 13 and 15 are directed to registering a secure domain name. This is done by verifying ownership information for an equivalent non-secure domain name corresponding to the secure domain name. The secure domain name is registered when the ownership information of the non-secure domain name is consistent with the ownership information for the secure domain name.

1.2 Thus, the application comprises two groups of independent claims having different features and based on different concepts.

Re Item V

Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

First Invention

1. Despite the above-clarity objections it appears that the subject-matter of Claim 1, understood as an apparatus claim, is not new, Article 33(2).

   D1 = DE A 199 24 575 is published earlier than the amended priority date of the application (26.04.2000). **D1** discloses an apparatus for providing a secure domain name service for a computer network and comprising a portal (30) connected to a computer network (col. 7, lines 10-16, col. 11, lines 34-39, fig. 1), the portal authenticating a query for a secure network address, and a domain name database (32) connected to the computer network through the portal, the domain name database storing secure computer network addresses (col. 10, lines 23-33, col. 12, lines 51-64).

2. All features of Claim 1 appear also to be known from **D2** = *DONALD E. EASTLAKE 3RD: '<draft-ietf-dnssec-secext2-05.txt> Domain Name System Security Extensions' INTERNET DRAFT, [Online] April 1998 (1998-04),* **XP002199931** *Retrieved from the Internet: <URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-dnssec-secext2-05.txt> [retrieved on 2002-05-23]*, see paragraph 2.4.

Second Invention

1. The subject-matter of Claim 13 is new and involves an inventive step, Article 33(2)(3).

1.1 Claim 13 is directed to a method for registering a secure domain name. The method comprises the steps of receiving a request and verifying ownership information for an equivalent non-secure domain name corresponding to the requested secure domain name. The secure domain name is registered in a secure domain name service when the ownership-information for the non-secure domain name is consistent with ownership information for the secure domain service.

This way of registration has the technical result that a client application accessing a non-secure web site can easily switch to the secure web site of the same owner by merely changing the top-level domain name without needing to change the whole domain name.

1.2 The above registration method is not suggested in the prior art.

JAMES E. BELLAIRE: 'Subject: New Statement of Rules - Naming Internet Domains ' INTERNET NEWSGROUP, [Online] 30 July 1995 (1995-07-30), **XP002209580** *comp.dcom.telecom Retrieved from the Internet: <URL:http://groups.google.com/> [retrieved on 2002-08-12]* does not relate to switching between a non-secure and a secure web site. The purpose of the document is to avoid potential trademark infringements. If the holder of a trademark provides evidence that an already assigned domain name is identical to that of the trademark, than the domain name will be put on hold until a court resolves the dispute. This also applies to the other documents cited in relation with the second invention.

2. The above finding also applies to Claim 15 which corresponds to Claim 13.

3. The dependent claims relate to specific embodiments of the above-mentioned independent claims and are therefore also new and inventive.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
23 August 2001 (23.08.2001)

PCT

(10) **International Publication Number**
WO 01/061922 A3

(51) **International Patent Classification⁷:** **H04L 12/56**, 29/06, 12/46

(21) **International Application Number:** PCT/US01/04340

(22) **International Filing Date:** 12 February 2001 (12.02.2001)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
09/504,783 15 February 2000 (15.02.2000) US

(63) **Related by continuation (CON) or continuation-in-part (CIP) to earlier application:**
US 09/504,783 (CON)
Filed on 15 February 2000 (15.02.2000)

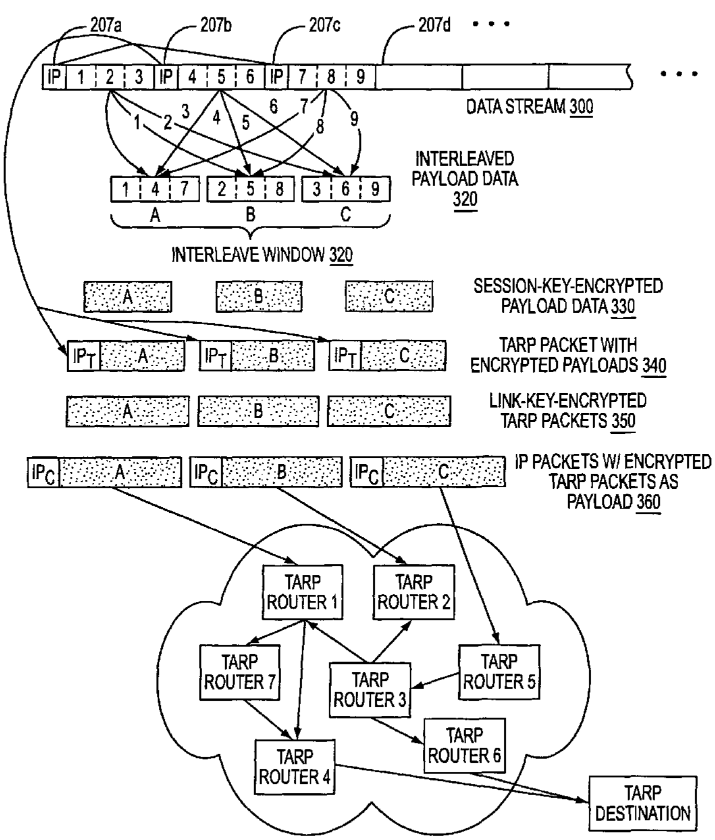
(71) **Applicant** *(for all designated States except US)*: **SCIENCE APPLICATIONS INTERNATIONAL CORPORATION** [US/US]; 10260 Campus Point Drive, San Diego, CA 92121 (US).

(72) **Inventors; and**
(75) **Inventors/Applicants** *(for US only)*: **MUNGER, Edmund, Colby** [US/US]; 1101 Opaca Court, Crownsville, MD 21032 (US). **SCHMIDT, Douglas, Charles** [US/US]; 230 Oak Court, Severna Park, MD 21146 (US). **SHORT, Robert, Dunham, III** [US/US]; 38710 Goose Creek Lane, Leesburg, VA 20175 (US). **LARSON, Victor** [US/US]; 12026 Lisa Marie Court, Fairfax, VA 22033 (US). **WILLIAMSON, Michael** [US/US]; 26203 Ocala Circle, South Riding, VA 20152 (US).

(74) **Agents: WRIGHT, Bradley, C.** et al.; Banner & Witcoff, Ltd., 11th Floor, 1001 G Street, N.W., Washington, DC 20001-4597 (US).

[Continued on next page]

(54) **Title:** AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY



(57) **Abstract:** A plurality of computer nodes communicate using seemingly random Internet Protocol source and destination addresses. Data packets matching criteria defined by a moving window of valid addresses are accepted for further processing, while those that do not meet the criteria are quickly rejected. Improvements to the basic design include (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities.

WO 01/061922 A3

(81) **Designated States** *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) **Date of publication of the international search report:**
6 March 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/04340

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/56 H04L29/06 H04L12/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 858 189 A (HITACHI LTD) 12 August 1998 (1998-08-12) column 6, line 35 -column 10, line 13 ---	1-27

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 August 2002	20. 08. 2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Ströbeck, A.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr al Application No
PCT/US 01/04340

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	MURTHY ET AL: "Congestion-oriented shortest multipath routing" PROCEEDINGS OF IEEE INFOCOM 1996. CONFERENCE ON COMPUTER COMMUNICATIONS. FIFTEENTH ANNUAL JOINT CONFERENCE OF THE IEEE COMPUTER AND COMMUNICATIONS SOCIETIES. NETWORKING THE NEXT GENERATION. SAN FRANCISCO, MAR. 24 - 28, 1996, PROCEEDINGS OF INFOCOM, L, vol. 2 CONF. 15, 24 March 1996 (1996-03-24), pages 1028-1036, XP010158171 ISBN: 0-8186-7293-5 abstract page 1028, left-hand column, line 38 -right-hand column, line 29 ---	1-27
E	WO 01 50688 A (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)) 12 July 2001 (2001-07-12) page 11, line 18 -page 13, line 21 ---	28,29,34
A	WO 98 59470 A (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)) 30 December 1998 (1998-12-30) page 4, line 5 -page 5, line 2 ---	28-39
X	WO 99 48303 A (CISCO TECHNOLOGY, INC.) 23 September 1999 (1999-09-23) page 1, line 8 -page 2, line 5 page 5, line 33 -page 6, line 15 page 7, line 21 - line 33	40,50
A	---	41-49, 51-59
A	JONES JIM ET AL: "Distributed Denial of Service Attacks: Defenses" INTERNET ARTICLE, 'Online! 2000, XP002208785 Retrieved from the Internet: <URL:www.bai.org/pdf/DDOS-defense.pdf > 'retrieved on 2002-08-05! paragraph '0005! ---	60-66
X	WO 99 38081 A (ASCEND COMMUNICATIONS INC) 29 July 1999 (1999-07-29) page 9, line 13 -page 10, line 17 page 11, line 10 -page 12, line 2	67
A	-----	68-71

International application No.
PCT/US 01/04340

INTERNATIONAL SEARCH REPORT

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. [X] As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

[X] No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-27

   A system and a method to balance the load between communication paths with varying transmission quality.

2. Claims: 28-39

   A system and a method to prevent someone from learning requested IP addresses by intercepting DNS requests.

3. Claims: 40-59

   A method to prevent a denial-of-service attack from an unauthenticated user flooding dummy data packets on to a low bandwidth link.

4. Claims: 60-66

   A method to prevent an authenticated user residing within a secure system from flooding it with dummy data packets.

5. Claims: 67-71

   A method to allocate memory in a central computer communicating with a potentially large number of client computers.

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte al Application No
PCT/US 01/04340

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
EP 0858189	A	12-08-1998	JP	10224400	A	21-08-1998
			EP	0858189	A2	12-08-1998
			US	6112248	A	29-08-2000
WO 0150688	A	12-07-2001	SE	517217	C2	07-05-2002
			AU	2564501	A	16-07-2001
			WO	0150688	A1	12-07-2001
			SE	9904841	A	30-06-2001
			US	2001006523	A1	05-07-2001
WO 9859470	A	30-12-1998	AU	8052398	A	04-01-1999
			SE	9702385	A	24-12-1998
			WO	9859470	A2	30-12-1998
WO 9948303	A	23-09-1999	AU	3098299	A	11-10-1999
			WO	9948303	A2	23-09-1999
WO 9938081	A	29-07-1999	US	6055575	A	25-04-2000
			AU	2562599	A	09-08-1999
			CA	2318267	A1	29-07-1999
			EP	1064602	A1	03-01-2001
			WO	9938081	A1	29-07-1999

Communication system using the internet

Patent number:	DE19924575 (A1)
Publication date:	1999-12-02
Inventor(s):	PROVINO JOSEPH E [US] +
Applicant(s):	SUN MICROSYSTEMS INC [US] +
Classification:	
- international:	***G06F13/00; H04L29/06; H04L29/12;*** **G06F13/00; H04L29/06; H04L29/12;** (IPC1-7): G06F12/14; G06F13/00; H04L12/22; H04L29/06; H04L9/00
- european:	H04L29/06; H04L29/06S2C; H04L29/12A2A1; H04L29/12A4A1B; H04L29/12A4A8B; H04L29/12A4A8D
Application number:	DE19991024575 19990528
Priority number(s):	US19980087823 19980529

Also published as:

- US6557037 (B1)
- JP2000049867 (A)
- GB2340702 (A)
- FR2782873 (A1)

Abstract of **DE 19924575 (A1)**

The system provides a connection between a virtual private network (15) and external units via the internet (14). The connection between the external units is made using a service provider (11). The virtual private network has a firewall (30) and internal servers (31) for secondary addresses and name addresses.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) Offenlegungsschrift

(10) DE 199 24 575 A 1

(51) Int. Cl.[6]:
H 04 L 29/06
H 04 L 12/22
G 06 F 13/00
G 06 F 12/14
// H04L 9/00

(21) Aktenzeichen: 199 24 575.4
(22) Anmeldetag: 28. 5. 99
(43) Offenlegungstag: 2. 12. 99

DE 199 24 575 A 1

(30) Unionspriorität:
087823 29. 05. 98 US

(71) Anmelder:
Sun Microsystems, Inc., Palo Alto, Calif., US

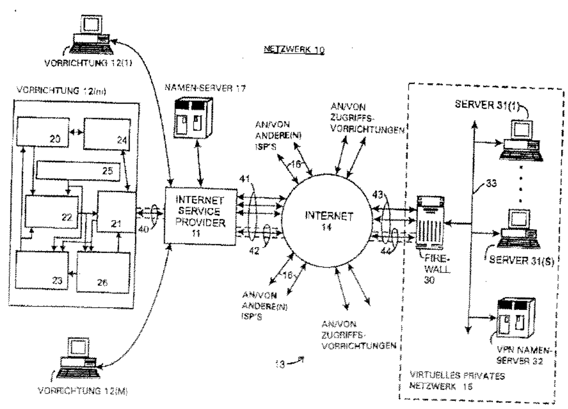
(74) Vertreter:
Samson & Partner, Patentanwälte, 80538 München

(72) Erfinder:
Provino, Joseph E., Cambridge, Mass., US

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Kommunikationssystem und -Verfahren

(57) Das erfindungsgemäße System umfaßt ein virtuelles privates Netzwerk (15) und eine externe Vorrichtung (12(m)), welche durch ein digitales Netzwerk (14) miteinander verbunden sind. Das virtuelle private Netzwerk (15) weist eine Firewall (30), wenigstens eine interne Vorrichtung (31(s)) und einen Namen-Server (32) auf, welche jeweils eine Netzwerkadresse besitzen. Die interne Vorrichtung (31(s)) besitzt auch eine Sekundäradresse, und der Namen-Server (32) ist derart konfiguriert, daß er eine Zuordnung zwischen der Sekundäradresse und der Netzwerkadresse bereitstellt. In Reaktion auf eine Anfrage von der externen Vorrichtung (12(m)) zum Aufbau einer Verbindung zur Firewall (30) übermittelt die Firewall (30) der externen Vorrichtung (12(m)) die Netzwerkadresse des Namen-Servers (32). In Reaktion auf eine Anfrage von einem Bediener oder ähnlichem, welche die Sekundäradresse der internen Vorrichtung (31(s)) enthält und einen Zugriff an die interne Vorrichtung (31(s)) anfordert, erzeugt die externe Vorrichtung (12(m)) eine Netzwerkadressen-Anfragenachricht zur Übertragung über die Verbindung an die Firewall (30), welche eine Auflösung der Netzwerkadresse, die der Sekundäradresse zugeordnet ist, anfordert. Die Firewall (30) übermittelt die Adressenauflösungsanfrage an den Namen-Server (32), und der Namen-Server (32) übermittelt die Netzwerkadresse, welche der Sekundäradresse zugeordnet ist, an die Firewall (30). Daraufhin stellt die Firewall (30) die Netzwerkadresse in einer ...



DE 199 24 575 A 1

Beschreibung

Die Erfindung betrifft allgemein das Gebiet der digitalen Kommunikationssysteme und -verfahren, und insbesondere Systeme und Verfahren zum Vereinfachen der Kommunikation zwischen Vorrichtungen, welche mit öffentlichen Netzwerken verbunden sind, z. B. dem Internet, und Vorrichtungen, welche mit privaten Netzwerken verbunden sind.

Digitale Netzwerke wurden entwickelt, um die Übertragung von Information, welche auch Daten und Programme umfaßt, über digitale Computersysteme und andere Digitalvorrichtungen zu ermöglichen. Es wurde eine Vielzahl von Arten von Netzwerken entwickelt und realisiert, einschließlich sog. Fernverbindungsnetze (Wide-Area Networks, nachfolgend "WAN" genannt) und lokale Netzwerke (Local Area Networks, nachfolgend "LAN" genannt), welche eine Information unter Verwendung verschiedener Informationsübertragungsmethoden übermitteln. Im allgemeinen werden LANs innerhalb kleiner geographischer Bereiche realisiert, z. B. innerhalb eines einzelnen Bürogebäudes oder ähnlichem, zum Übertragen von Information innerhalb eines bestimmten Büros, einer Firma oder einer ähnlichen Art von Organisationseinheit. Andererseits werden WANs im allgemeinen auf relativ großen geographischer Bereichen realisiert und können verwendet werden, um Information sowohl zwischen LANs als auch zwischen Vorrichtungen, welche nicht mit LANs verbunden sind, zu übertragen. Derartige WANs umfassen auch öffentliche Netzwerke, z. B. das Internet, welche zur Informationsübertragung zwischen einer Anzahl von Unternehmen verwendet werden können.

Es sind mehrere Probleme im Zusammenhang der Kommunikation über ein Netzwerk aufgetreten, insbesondere in einem großen öffentlichen WAN, wie es z. B. das Internet ist. Im allgemeinen werden Informationen über ein Netzwerk in Nachrichtenpaketen übertragen, welche ausgehend von einer Vorrichtung, als Quelle bzw. Quellenvorrichtung, zu einer anderen Vorrichtung, als Ziel bzw. Zielvorrichtung, über einen oder mehrere Router oder allgemein Schaltungsknoten im Netzwerk übertragen werden. Jedes Nachrichtenpaket enthält eine Zieladresse, welche von den Schaltungsknoten verwendet wird, um das jeweilige Nachrichtenpaket an die geeignete Zielvorrichtung zu leiten. Z.B. im Internet haben solche Adressen die Form von "n"-Bit Zahlen (wobei "n" 32 oder 128 sein kann), wobei solche Zahlenkolonnen für einen Benutzer schwierig sind zu merken und einzugeben, wenn die oder der Benutzer die Übertragung eines Nachrichtenpakets veranlassen möchte. Um einen Benutzer von der Notwendigkeit zu befreien, sich solche spezifische Zahlen-Internetadressen zu merken und einzugeben, stellt das Internet einen zweiten Adressierungsmechanismus bereit, der durch Benutzer der jeweiligen Vorrichtungen einfacher handzuhaben ist. Bei diesem Adressierungsmechanismus werden Internet-Domains, wie etwa LANs, Internet-Service-Provider (nachfolgend "ISP" genannt) und ähnliche, welche im Internet verbunden sind, durch für einen Benutzer relativ einfach les- und merkbare Namen identifiziert, die nachfolgend als "Klartextnamen" bezeichnet werden. Um den Einsatz von solchen Klartextnamen umzusetzen, werden Namen-Server, auch als DNS-Server für "Domain Name Server" bezeichnet, bereitgestellt, um die Klartextnamen in die geeigneten Internetadressen umzuwandeln. Wenn ein Bediener einer Vorrichtung, der die Übertragung eines Nachrichtenpakets an eine andere Vorrichtung wünscht, den Klartextnamen der anderen Vorrichtung eingibt, nimmt die Vorrichtung zuerst Kontakt mit einem Namen-Server auf. Im allgemeinen kann der Namen-Server ein Teil des ISP selbst sein oder er kann eine spezielle Vorrichtung sein, welche durch den ISP über das Internet zugänglich ist; in jedem Fall wird der ISP den Namen-Server identifizieren, welcher für die Vorrichtung zu verwenden ist, wenn sich die Vorrichtung beim ISP einloggt, d. h. anmeldet. Falls der Namen-Server, nachdem die Vorrichtung einen Kontakt hergestellt hat, eine Zahlen-Internetadresse für den Klartext-Domainnamen besitzt oder erhalten kann, übermittelt der Namen-Server die Zahlen-Internetadresse, welche dem Klartext-Domainnamen entspricht, zu der Vorrichtung des Bedieners. Die Vorrichtung kann sodann die Zahlen-Internetadresse, welche von dem Namen-Server zurückgesendet wurde, in das Nachrichtenpaket einfügen und das Nachrichtenpaket an den ISP für die Übertragung über das Internet auf konventioneller Weise liefern. Die Internet-Schaltungsknoten verwenden die Zahlen-Internetadresse, um das Nachrichtenpaket an die gewünschte Zielvorrichtung zu übermitteln.

Andere Probleme treten insbesondere in Verbindung mit der Übertragung von Information über ein öffentliches WAN, z. B. das Internet, auf. Ein Problem besteht darin, sicherzustellen, daß die über das WAN übertragene Information, welche die Quellenvorrichtung und die Zielvorrichtung vertraulich behalten möchten, auch tatsächlich vertraulich bleibt gegenüber möglichen Lauschern, welche die Information abfangen können. Um die Vertraulichkeit zu wahren, wurden verschiedene Formen von Verschlüsselung entwikkelt und werden verwendet, um die Information vor der Übertragung durch die Quellenvorrichtung zu verschlüsseln und die Information nach deren Empfang durch die Zielvorrichtung zu entschlüsseln. Falls gewünscht wird, daß beispielsweise die gesamte Information, welche zwischen einer bestimmten Quellenvorrichtung und einer bestimmten Zielvorrichtung übertragen wird, vertraulich bleiben soll, können die Vorrichtungen einen sog. "Sicherheitstunnel" zwischen den Vorrichtungen einrichten, der im wesentlichen sicherstellt, daß die gesamte Information, welche von der Quellenvorrichtung an die Zielvorrichtung übertragen wird, vor der Übertragung verschlüsselt wird (mit Ausnahme von bestimmten Protokollinformationen, wie Adresseninformation, welche den Fluß von Netzpaketen über das Netzwerk zwischen der Quellen- und Zielvorrichtung steuert), und daß die verschlüsselte Information vor der Verwendung durch die Zielvorrichtung entschlüsselt wird. Die Quellen- und Zielvorrichtungen können jeweils für sich eine Verschlüsselung bzw. Entschlüsselung durchführen, oder die Verschlüsselung und Entschlüsselung kann durch andere Vorrichtungen durchgeführt werden, bevor die Nachrichtenpakete über das Internet übertragen werden.

Ein weiteres Problem, welches insbesondere im Zusammenhang mit Unternehmen, Regierungsämtern und privaten Organisationen auftritt, deren private Netzwerke, welche LANs, WANs oder etwaige Kombinationen derselben sein können, mit öffentlichen WANs, z. B. dem Internet, verbunden sind, besteht darin, sicherzustellen, daß deren private Netzwerke sicher sind gegenüber anderen Netzwerken, zu welchen z. B. die Unternehmen keinen Zugriff haben möchten, oder einen Zugriff durch andere zu regulieren und zu kontrollieren, zu welchen z. B. die jeweiligen Organisationen einen begrenzten Zugriff haben möchten. Um dies umzusetzen, verbinden die Organisationen in der Regel ihre privaten Netzwerke mit öffentlichen WANs über eine begrenzte Anzahl von Gateways, welche manchmal als "Firewalls" bezeichnet werden, durch welche der gesamte Netzverkehr zwischen dem internen und dem öffentlichen Netzwerk läuft. In der Regel sind Netzwerkadressen von Domains und Vorrichtungen in dem privaten Netzwerk "hinter" der Firewall den Namen-Servern bekannt, welche in den privaten Netzwerken vorgesehen sind; sie sind aber nicht zugänglich für Namen-Server oder andere Vorrichtungen außerhalb der privaten Netzwerke, was die Kommunikation zwischen einer Vorrichtung außerhalb des privaten Netzwerkes und einer Vorrichtung innerhalb des privaten Netzwerkes schwierig macht.

Ein Ziel der vorliegend Erfindung ist es, hier Abhilfe zu schaffen.

Dieses Ziel erreicht die Erfindung durch die Gegenstände der Ansprüche 1, 7 und 13. Bevorzugte Ausführungsbeispiele der Erfindung sind in den jeweils abhängigen Ansprüchen beschrieben.

Danach schafft die Erfindung ein neuartiges und verbessertes System und ein Verfahren zum Vereinfachen von Kommunikation zwischen Vorrichtungen, welche mit öffentlichen Netzwerken, z. B. dem Internet, verbunden sind, und Vorrichtungen, welche mit privaten Netzwerken verbunden sind, wobei die Auflösung von Sekundäradressen, wie etwa Text- bzw. Klartextnamen im Internet, in die zugehörigen Netzwerkadressen durch Namen-Server oder ähnliche Vorrichtungen, die mit den privaten Netzwerken verbunden sind, ermöglicht wird.

Hierfür stellt die Erfindung ein System zur Verfügung mit einem virtuellen Privaten Netzwerk und einer externen Vorrichtung, welche durch ein digitales Netzwerk miteinander verbunden sind, sowie ein Kommunikationsverfahren und ein Computerprogrammprodukt zum gemeinsamen Verwenden mit einem derartiges System. Das virtuelle private Netzwerk weist eine Firewall bzw. ein Firewall-System, wenigstens eine interne Vorrichtung und einen Namen-Server auf, welche jeweils eine Netzwerkadresse besitzen. Die interne Vorrichtung besitzt ferner eine Sekundäradresse, und der Namen-Server ist derart konfiguriert, daß er eine Zuordnung zwischen der Sekundäradresse und der Netzwerkadresse bereitstellt. In Reaktion auf eine Anfrage von der externen Vorrichtung zum Aufbau einer Verbindung zur Firewall übermittelt die Firewall der externen Vorrichtung die Netzwerkadresse des Namen-Servers. In Reaktion auf eine Anfrage von einem Bediener oder ähnlichem, welche die Sekundäradresse der internen Vorrichtung enthält und einen Zugriff an die interne Vorrichtung anfordert, erzeugt die externe Vorrichtung eine Netzwerkadressen-Anfragenachricht zur Übertragung über die Verbindung an die Firewall, welche eine Auflösung der Netzwerkadresse, die der Sekundäradresse zugeordnet ist, anfordert. Die Firewall übermittelt die Adressenauflösungsanfrage an den Namen-Server und der Namen-Server übermittelt die Netzwerkadresse, welche der Sekundäradresse zugeordnet ist, an die Firewall. Daraufhin stellt die Firewall die Netzwerkadresse in einer Netzwerkadressenantwortnachricht zur Übertragung über die Verbindung an die externe Vorrichtung bereit. Die externe Vorrichtung kann sodann die auf diese Weise bereitgestellte Netzwerkadresse in nachfolgenden an die interne Vorrichtung gerichtete Kommunikationen mit der Firewall verwenden.

Weitere Vorteile und Ausgestaltungen der Erfindung ergeben sich aus der nachfolgenden detaillierten Beschreibung eines bevorzugten Ausführungsbeispiels. In der Beschreibung wird auf die beigefügte schematische Zeichnung Bezug genommen. Darin zeigt:

Fig. 1 ein funktionelles Blockdiagramm eines erfindungsgemäßen Netzwerkes.

Fig. 1 zeigt ein funktionelles Blockdiagramm eines Netzwerkes **10**, welches gemäß der vorliegenden Erfindung aufgebaut ist. Das Netzwerk **10** gemäß **Fig.** 1 umfaßt einen Internet-Service-Provider (nachfolgend "ISP") **11**, welcher die Übertragung von Nachrichtenpaketen zwischen einer oder mehreren Vorrichtungen **12(1)** bis **12**(M) (nachfolgend allgemeinen mit dem Bezugszeichen **12**(m) identifiziert), welche mit dem ISP **11** verbunden sind, und anderen Vorrichtungen, welche allgemein durch ein Bezugszeichen **13** gekennzeichnet sind, über das Internet **14** ermöglicht, wobei die Übertragung von Information in Nachrichtenpaketen zwischen den Vorrichtungen **12**(m) und **13** realisiert wird. Der ISP **11** verbindet das Internet **14** über eine oder mehrere logische Verbindungen oder Gateways oder ähnlichem (im vorliegenden allgemein als "Verbindungen" bezeichnet), welche allgemein durch das Bezugszeichen **41** gekennzeichnet sind. Der ISP **11** kann ein öffentlicher ISP sein, welcher in diesem Falle die Verbindung mit Vorrichtungen **12**(m) herstellt, welche durch Bediener betrieben werden können, die der allgemeinen Öffentlichkeit angehören, so daß diese Bediener Zugang zu dem Internet erlangen. Alternativ dazu kann der ISP **11** ein privater ISP sein. In diesem Falle werden die damit verbundenen Vorrichtungen **12**(m) im allgemeinen beispielsweise durch Angestellte eines bestimmten Unternehmens oder einer Regierungseinrichtung, Mitgliedern von einer privaten Organisation oder ähnlichen betrieben, um diesen Angestellten oder Mitglieder einen Zugang in das Internet bereit zu stellen.

In an sich konventioneller Weise weist das Internet ein Netz von Schaltungsknoten auf (welche nicht separat dargestellt sind), welche die ISPs **11** und die Vorrichtungen **13** miteinander verbinden, um dazwischen die Übertragung von Nachrichtenpaketen zu ermöglichen. Die Nachrichtenpakete, welche über das Internet **14** übertragen werden, stimmen mit denjenigen überein, welche durch das sog. Internetprotokoll (IP) definiert werden, und umfassen einen Kopfabschnitt, einen Datenabschnitt und können einen Fehlererfassungs- und/oder Korrekturabschnitt aufweisen. Der Kopfabschnitt enthält Information, welche verwendet wird, um das Nachrichtenpaket über das Internet **14** zu übertragen, beispielsweise eine Zieladresse, welche die Vorrichtung identifiziert, welche das Nachrichtenpaket als Zielvorrichtung empfangen soll, und eine Quellenadresse, welche diejenige Vorrichtung identifiziert, welche das Nachrichtenpaket erzeugt hat. In jedem Nachrichtenpaket haben die Ziel- und Quellenadresse jeweils die Form einer Zahl, welche eindeutig die jeweilige Ziel- bzw. Quellenvorrichtung identifiziert. Die Schaltungsknoten im Internet **14** verwenden wenigstens die Zieladresse eines jeweiligen Nachrichtenpaketes, um das jeweilige Nachrichtenpaket an die Zielvorrichtung zu übermitteln, wenn die Zielvorrichtung an das Internet angeschlossen ist, oder an einen ISP **11** oder andere Vorrichtungen, welche an das Internet **14** angeschlossen sind, welche sodann das Nachrichtenpaket an das geeignete Ziel senden werden. Der Datenabschnitt eines jeden Nachrichtenpakets enthält die in dem Nachrichtenpaket übertragenen Daten; und der Fehlererfassungs- und/oder Korrekturabschnitt enthält Fehlererfassungs- und/oder Korrekturinformationen, welche verwendet werden können, um zu verifizieren, daß das Nachrichtenpaket in korrekter Weise von der Quelle zu der Zielvorrichtung übertragen wurde (im Fall der Fehlererfassungsinformation), und um ausgewählte Arten von Fehlern zu korrigieren, falls das Nachrichtenpaket nicht korrekt übertragen wurde (im Falle der Fehlerkorrekturinformation).

Die Vorrichtungen **12**(m), welche mit dem ISP **11** verbunden sind, können jede beliebige Anzahl von Arten von Vorrichtungen umfassen, welche über das Internet **14** mit anderen Vorrichtungen **13** kommunizieren, umfassend z. B. Personalcomputer, Computer-Workstations und ähnliches. Jede Vorrichtung **12**(m) kommuniziert mit dem ISP **11**, um Nachrichtenpakete für die Übertragung über das Internet **14** an diesen zu übertragen, oder um Nachrichtenpakete, welche durch den ISP **11** über das Internet empfangen werden, von diesem zu empfangen. Dabei kann jedes geeignete Protokoll verwendet werden, z. B. das bekannte Point-to-Point Protokoll (allgemein mit "PPP" abgekürzt), falls die Vorrichtung **12**(m) über eine Point-to-Point Verbindung mit dem ISP **11** verbunden ist, oder irgendein konventionelles "Multi-Drop" Protokoll, falls die Vorrichtung **12**(m) mit dem ISP **11** über ein "Multi-Drop"-Netzwerk, z. B. das Ethernet, verbunden ist, oder ähnliches. Die Vorrichtungen **12**(m) sind im allgemeinen entsprechend der üblichen Computerarchitektur mit gespeicherten Programmen aufgebaut, welche z. B. eine Systemeinheit, eine Bildschirmanzeigeeinheit und Bedienereingabeeinrichtungen, wie etwa eine Tastatur oder eine Maus, umfaßt. Eine Systemeinheit weist im allgemeinen eine oder mehrere Prozessor-, Speicher-, Massenspeichereinrichtungen, z. B. Festplatten- und/oder Bandspeicherelemente, oder andere Elemente (nicht separat gezeigt) auf, wie etwa Netzwerk- und/oder Telephonschnittstelleneinrichtungen, um die jeweilige Vorrichtung an den ISP **11** anzukoppeln. Die Prozessor- bzw. Verarbeitungseinrichtungen verarbeiten Programme, einschließlich Anwendungsprogramme, unter der Steuerung eines Betriebssystems, um verarbeitete Daten zu erzeugen. Die Bildschirmeinheit ermöglicht es der Vorrichtung, die verarbeiteten Daten und einen Verarbeitungsstatus der Daten dem Benutzer anzuzeigen, und die Bedienereingabeeinrichtung ermöglicht es dem Bediener, Daten einzugeben und die Verarbeitung zu steuern.

Diese Elemente der Vorrichtung **12**(m) arbeiten in Verbindung mit einer geeigneten Programmierung so zusammen, um eine Vorrichtung **12**(m) mit einer Anzahl von funktionellen Elementen bereit zustellen, beispielsweise eine Bedienerschnittstelle **20**, eine Netzwerkschnittstelle **21**, einen Nachrichtenpaketgenerator **22**, einen Nachrichtenpaketempfänger und -prozessor **23**, eine ISP Einloggsteuerung bzw. Anmeldungssteuerung **24**, einen Internetparameterspeicher **25** und im Zusammenhang mit der vorliegenden Erfindung einen Sicherheits-Nachrichtenpaketprozessor **26**. Die Bedienerschnittstelle **20** ermöglicht, daß die Vorrichtung **12**(m) Eingabeinformationen von der/den Bedienereingabevorrichtung(en) der Vorrichtung **12**(m) empfängt und die Ausgabeinformationen dem Bediener auf der/den Bildschirmeinrichtung(en) der Vorrichtung **12**(m) angezeigt werden. Die Netzwerkschnittstelle **21** ermöglicht eine Verbindung der Vorrichtung **12**(m) mit dem ISP **11** unter Verwendung des geeigneten PPP oder Netzwerkprotokolls, um Nachrichtenpakete an den ISP **11** zu übertragen und von diesem Nachrichtenpakete zu empfangen. Die Netzwerkschnittstelle **21** kann eine Verbindung mit dem ISP **11** über das öffentliche Telefonnetz vorsehen, um einen Wählverbindungsnetzwerkbetrieb (sog. Dial-Up Betrieb) der Vorrichtung **12**(m) über das öffentliche Telefonnetz zu ermöglichen. Alternativ oder zusätzlich dazu kann die Netzwerkschnittstelle **21** eine Verbindung durch den ISP **11** über beispielsweise ein konventionelles LAN ermöglichen, wie etwa das Ethernet. In Reaktion auf eine durch die Bedienerschnittstelle **20** gelieferte Eingabe und/oder in Reaktion auf Anfragen aus Programmen (nicht gezeigt), welche durch die Vorrichtung **12**(m) verarbeitet werden, kommuniziert die ISP Einloggsteuerung **24** über die Netzwerkschnittstelle **21**, um die Initialisierung (sog. "Log-On") einer Kommunikationssitzung zwischen der Vorrichtung **12**(m) und dem ISP **11** zu ermöglichen. Während dieser Kommunikationssitzung kann die Vorrichtung **12**(m) Information in der Form von Nachrichtenpaketen an andere Vorrichtungen über das Internet **14** sowie an andere Vorrichtungen **12**(m') (wobei m' ≠ m), welche mit der ISP **11** oder mit anderen ISPs verbunden sind, übertragen. Während eines Log-On-Betriebs empfängt die ISP Einloggsteuerung **24** die Internetprotokollparameter (IP-Parameter), welche im Zusammenhang mit einer Nachrichtenpaketerzeugung während der Kommunikationssitzung verwendet werden.

Während einer Kommunikationssitzung erzeugt der Nachrichtenpaketgenerator **22** Nachrichtenpakete zur Übertragung durch die Netzwerkschnittstelle **21** in Reaktion auf eine Eingabe, welche durch den Bediener über die Bedienerschnittstelle **20** geliefert wird und/oder in Reaktion auf Anfragen aus Programmen (nicht separat gezeigt), welche durch die Vorrichtung **12**(m) verarbeitet werden. Die Netzwerkschnittstelle **21** empfängt auch Nachrichtenpakete aus dem ISP **11** und liefert diese an den Nachrichtenpaketempfänger und -prozessor **23** zur Verarbeitung und Bereitstellung an die Bedienerschnittstelle **20** und/oder anderen Programmen (nicht gezeigt), welche durch die Vorrichtung **12**(m) verarbeitet werden. Falls die empfangenen Nachrichtenpakete eine Information enthalten, z. B. Web-Seiten oder ähnliches, welche dem Bediener angezeigt werden soll, kann die Information der Bedienerschnittstelle **20** geliefert werden, damit die Information auf der Bildschirmeinheit der Vorrichtung angezeigt wird. Zusätzlich oder alternativ dazu kann die Information an andere Programme (nicht gezeigt) zur Verarbeitung geliefert werden, welche durch die Vorrichtung **12**(m) verarbeitet werden.

Im allgemeinen können die Elemente, wie die Bedienerschnittstelle **20**, der Nachrichtenpaketgenerator **22**, der Nachrichtenpaketempfänger und -prozessor **23**, die ISP Einloggsteuerung **24** und der Internetparameterspeicher **25** Elemente eines konventionellen Internet-Browsers enthalten, wie die von Mosaic, Netscape Navigator und Microsoft Internet Explorer.

Wie es oben erwähnt wurde, weist die Vorrichtung **12**(m) im Zusammenhang mit der vorliegenden Erfindung einen Sicherheits-Nachrichtenpaketprozessor **26** auf. Der Sicherheits-Nachrichtenpaketprozessor **26** ermöglicht den Aufbau und Verwendung eines "Sicherheitstunnels" zwischen der Vorrichtung **12**(m) und anderen Vorrichtungen **12**(m') (wobei m' ≠ m) oder **13**, wie es welches weiter unten beschrieben wird. Im allgemeinen wird in einem solchen Sicherheitstunnel Information in wenigstens dem Datenabschnitt der zwischen der Vorrichtung **12** (m) und einer spezifischen anderen Vorrichtung **12**(m') (wobei m' ≠ m) oder **13** übertragenen Nachrichtenpakete geheimgehalten, beispielsweise durch Verschlüsselung des Datenabschnittes vor der Übertragung durch die Quellenvorrichtung. Die Information in anderen Abschnitten eines derartigen Nachrichtenpakets kann ebenfalls geheimgehalten werden, mit Ausnahme der Information, welche benötigt wird, um die Übertragung des jeweiligen Nachrichtenpakets zwischen den Vorrichtungen zu ermöglichen, also z. B. wenigstens die Zielinformation, damit die Schaltungsknoten des Internets und die ISPs die Vorrichtung identifizieren können, welche das Nachrichtenpaket empfangen soll.

Zusätzlich zu dem ISP **11** kann eine Vielzahl von anderen ISPs die Verbindung zum Internet herstellen, wie es durch die Pfeile **16** angedeutet ist, um eine Kommunikation zwischen Vorrichtungen, welche an diesen anderen ISPs angeschlossen sind, mit anderen Vorrichtungen über das Internet zu ermöglichen, welche die Vorrichtungen **12**(n), welche an dem ISP **11** angeschlossen sind, umfassen können.

Die Vorrichtungen **13**, auf welche die Vorrichtungen **12**(m) zugreifen und mit welchen diese kommunizieren, können auch von jeder beliebigen Anzahl von Arten von Vorrichtungen sein, einschließlich Personalcomputer, Computer-Workstations und ähnliches, oder auch Minicomputer und Großrechner, Großspeichersysteme, Rechenserver, lokale Netzwerke (LANs) und Fernverbindungsnetzwerke (WANs), welche derartige Vorrichtungen und zahlreiche andere Arten von Vorrichtungen enthalten, die direkt oder indirekt mit den Netzwerken verbunden werden können. Nach der vorliegenden Erfindung umfaßt wenigstens eine der Vorrichtungen wenigstens ein privates Netzwerk, welches als virtuelles privates Netzwerk **15** gekennzeichnet ist und z. B. die Form eines LAN oder eines WAN haben kann. Das virtuelle private Netzwerk **15** kann jede der Vorrichtungen **12**(m') (wobei m' ≠ m) aufweisen (wobei die Verbindung zu dem Internet **14** über einen ISP erfolgt) oder der Vorrichtungen **13** (wobei die Verbindung zu dem Internet **14** unmittelbar erfolgt). Bei dem vorliegend beschriebenen Ausführungsbeispiel wird angenommen, daß das virtuelle Netzwerk **15** eine Vorrichtung **13** aufweist. Das virtuelle private Netzwerk **15** umfaßt selbst mehrere Vorrichtungen, welche hier als eine Firewall bzw. ein Firewall-System **30**, mehrere Server **31**(**1**) bis **31**(S) (im nachfolgenden allgemein mit dem Bezugszeichen **31**(s) angegeben) und ein Namen-Server **32** gekennzeichnet sind, wobei allesamt durch eine Übertragungsverbindung **33** miteinander verbunden sind. Die Firewall **30** und die Server **31**(s) können ähnlich sein wie jede der verschiedenen Arten von Vorrichtungen **12**(m) und **13**, die hier beschrieben sind, und können daher beispielsweise umfassen Personalcomputer, Computer-Workstations und ähnliches, aber auch Minicomputer und Großrechner, Großspeichersysteme, Rechenserver, lokale Netzwerke (LANs) und Fernverbindungsnetzwerke (WANs), welche derartige Vorrichtungen und zahlreiche andere Arten von Vorrichtungen umfassen, welche direkt oder indirekt mit den Netzwerken verbunden werden können.

Wie oben ausgeführt wurde, kommunizieren diese Vorrichtungen einschließlich der Vorrichtungen **12**(m) und der Vorrichtungen **13** durch Übertragung von Nachrichtenpaketen über das Internet. Die Vorrichtungen **12**(m) und **13** können Information in einem Peer-to-Peer bzw. gleichrangigem Modus, in einem Client-Server Modus oder nach beiden dieser Modi übertragen. Im allgemeinen überträgt eine Vorrichtung in einer Peer-to-Peer Nachrichtenpaketübertragung Information in einem oder mehreren Nachrichtenpaketen an die andere Vorrichtung. Andererseits kann eine Vorrichtung, welche in einem Client-Server Modus als Client fungiert, ein Nachrichtenpaket an eine andere Vorrichtung übertragen, welche als Server fungiert, um beispielsweise einen Dienst durch die andere Vorrichtung auszulösen. Mehrere Arten derartiger Dienste sind dem Fachmann bekannt, beispielsweise das Wiedergewinnen bzw. Auslesen von Information aus der anderen Vorrichtung, damit diese aktiviert wird, um Verarbeitungsoperationen und dergleichen durchzuführen. Falls der Server dazu dient, dem Client vor allem Informationen zu liefern, kann dieser allgemein als ein Speicherserver bezeichnet werden. Falls der Server andererseits Verarbeitungsoperationen auf Anfrage des Client ausführen soll, kann dieser allgemein als ein Rechnerserver bezeichnet werden. Andere Arten von Servern zum Ausführen von anderen Arten von Diensten und Operationen auf Anfrage von Clients sind dem Fachmann ebenfalls bekannt.

Wenn in einer Client-Server Anordnung eine Vorrichtung **12**(m) einen Dienst durch beispielsweise eine Vorrichtung **13** ausgeführt haben möchte, erzeugt die Vorrichtung **12**(m) eines oder mehrere Anfragenachrichtenpakete zur Übertragung an die Vorrichtung **13**, welche den benötigten Dienst anfordern. Das Anfragenachrichtenpaket enthält die Internetadresse der Vorrichtung **13**, welche als die Zielvorrichtung das Nachrichtenpaket empfängt und den Dienst ausführt. Die Vorrichtung **12** (m) überträgt das/die Anfragenachrichtenpaket(e) an den ISP **11**. Der ISP **11** überträgt daraufhin das Nachrichtenpaket über das Internet an die Vorrichtung **13**.

Falls die Vorrichtung **13** die Form eines WAN oder LAN hat, empfängt das WAN oder LAN das/die Nachrichtenpaket(e) und leitet dieses/diese zu einer dort angeschlossenen Vorrichtung weiter, welche den angeforderten Dienst ausführen soll.

In jedem Fall wird die Vorrichtung **13**, welche den angeforderten Dienst ausführen soll, nach Empfang des/der Anfragenachrichtenpaket(e) die Anfrage bearbeiten. Falls die Vorrichtung **12**(m), welche das/die Anfragenachrichtenpaket(e) erzeugt hat, oder deren Bediener die notwendigen Befugnisse hat, um den Dienst von der Vorrichtung **13** anzufordern, und falls der angeforderte Dienst die Einleitung einer Informationsübertragung aus der Vorrichtung **13** als ein Speicherserver an die Vorrichtung **12**(m) als ein Client umfaßt, erzeugt die Vorrichtung **13** eines oder mehrere Antwortnachrichtenpakete, welche die angeforderten Informationen enthalten, und überträgt das/die Paket(e) über das Internet **14** an den ISP **11**. Daraufhin überträgt der ISP **11** das/die Nachrichtenpaket(e) an die Vorrichtung **12**(m). Falls andererseits der angeforderte Dienst die Einleitung eines Verarbeitungsvorganges durch die Vorrichtung **13** als ein Rechenserver beinhaltet, wird die Vorrichtung **13** den/die angeforderten Rechendienst(e) ausführen. Falls die Vorrichtung **13** verarbeitete Daten, welche während den Rechenvorgängen erzeugt wurden, an die Vorrichtung **12**(m) als Client zurücksenden soll, erzeugt die Vorrichtung **13** zusätzlich eines oder mehrere Antwortnachrichtenpakete, welche die verarbeiteten Daten enthalten und überträgt das/die Paket(e) über das Internet **14** an den ISP **11**. Der ISP **11** überträgt daraufhin das/die Nachrichtenpaket(e) an die Vorrichtung **12**(m). Entsprechende Operationen können durch die Vorrichtungen **12**(m) und **13**, dem ISP **11** und dem Internet **14** in Verbindung mit anderen Arten von Diensten ausgeführt werden, welche durch die Server-Vorrichtungen **13** bereitgestellt werden können.

Wie oben angemerkt wurde, enthält jedes Nachrichtenpaket, welches durch die Vorrichtungen **12**(m) und **13** zur Übertragung über das Internet **14** erzeugt wird, eine Zieladresse,welche von den Schaltungsknoten verwendet wird, um das jeweilige Nachrichtenpaket an die geeignete Zielvorrichtung zu leiten. Adressen im Internet haben die Form von "n"-Bit Zahlen (wobei "n" beim gegenwärtigen Standard **32** oder **128** sein kann). Um insbesondere einen Bediener einer Vorrichtung **12**(m) von der Notwendigkeit zu befreien, sich spezifische Zahlenkolonnen bzw. Zahlen-Internetadressen zu merken und diese der Vorrichtung **12**(m) einzugeben, um die Erzeugung eines Nachrichtenpakets zur Übertragung über das Internet einzuleiten, stellt das Internet einen zweiten Adressierungsmechanismus zur Verfügung, welcher einfacher durch menschliche Bediener der jeweiligen Vorrichtungen handhabbar ist. Bei diesem Adressierungsmechanismus werden Internet-Domains, wie etwa LANs, Internet-Service-Provider (ISPs) und ähnliche, welche in bzw. mit dem Internet verbunden sind, durch relativ einfach les- und merkbare Namen, sog. Klartextnamen, identifiziert. Dabei soll sich hier die Bezeichnung "Klartextname" auf jede Art von Namenstext beziehen, z. B. auch auf Abkürzungen, generische Bezeichnungen, Phantasiebegriffe, etc. Um das System der Klartext-Domainnamen umzusetzen, ist der ISP **11** mit einem Namen-Server **17** (der auch als ein DNS Server (Domain Name Server) bezeichnet werden kann) verbunden, welcher die Klartext-Domainnamen auflösen bzw. in eine gültige Internetadresse umwandeln kann, um die geeignete Internetadresse für das in dem jeweiligen Klartextnamen angegebene Ziel bereitzustellen. Im allgemeinen kann der Namen-Server ein Teil des ISP **11** oder damit direkt verbunden sein, wie es in **Fig.** 1 gezeigt ist, oder er kann eine bestimmte Vorrichtung sein, welche durch den ISP über das Internet zugänglich ist. Jedenfalls wenn sich die Vorrichtung **12**(m) bei dem ISP **11** während einer Kommunikationssitzung einloggt, wird der ISP **11**, wie oben hingewiesen wurde, verschiedene Internet-Protokollparameter (IP-Parameter) zuordnen, welche die Vorrichtung 12(m) während der Kommunikationssitzung verwendet, und welche in dem Internetparameterspeicher 25 gespeichert sind. Diese IP-Parameter enthalten Informationen, wie

(a) eine Internetadresse für die Vorrichtung 12(m), welche die Vorrichtung 12(m) während der Kommuniationssitzung identifiziert; und

(b) die Identifizierung eines Namen-Servers 17, welchen die Vorrichtung 12(m) während der Kommunikationssitzung verwendet.

Wenn die Vorrichtung 12(m) Nachrichtenpakete zur Übertragung erzeugt, fügt sie ihre Internetadresse (obiger Punkt (a)) als die Quellenadresse ein. Die Vorrichtung(en) 13, welche die jeweiligen Nachrichtenpakete empfängt/empfangen, kann/können die Quellenadresse aus den Nachrichtenpaketen, welche von der Vorrichtung 12(m) empfangen werden, in Nachrichtenpaketen verwenden, welche die Vorrichtung(en) 13 zur Übertragung an die Vorrichtung 12(m) erzeugt/erzeugen, so daß das Internet in der Lage ist, die durch die jeweilige Vorrichtung 13 erzeugten Nachrichtenpakete an die Vorrichtung 12(m) zu leiten. Falls die Vorrichtung 12(m) auf den Namen-Server 17 über das Internet 14 zugreift, hat die durch den ISP 11 bereitgestellte Identifizierung des Namen-Servers 17 (siehe oben unter (b)) die Form einer Zahlen-Internetadresse, welche es der Vorrichtung 12(m) ermöglicht, für den Namen-Server 17 Nachrichten zu erzeugen, welche eine Auflösung der Klartext-Internetadressen in Zahlen-Internetadressen anfordern. Der ISP 11 kann der Vorrichtung 12(m) auch andere IP-Parameter zuordnen, wenn diese sich beim ISP 11 einloggt, beispielsweise die Identifizierung einer Verbindung zu dem Internet 14, welche für Nachrichten zu verwenden ist, die durch die Vorrichtung 12(m) übersandt werden, insbesondere falls der ISP 11 Mehrfach-Gateways aufweist. In der Regel speichert die Vorrichtung 12(m) die Internetparameter im Internetparameterspeicher 25 für die Verwendung während der Kommunikationssitzung.

Wenn ein Bediener die Vorrichtung 12(m) veranlassen möchte, daß sie ein Nachrichtenpaket an eine Vorrichtung 13 überträgt gibt der oder die Bediener(in) die Internetadresse der Vorrichtung 13 an die Vorrichtung 12(m) über die Bedienerschnittstelle 20 ein, sowie eine Information oder die Identifizierung der in der Vorrichtung 12(m) aufbewahrten Information, welche in der Nachricht überragen werden sollen. Die Bedienerschnittstelle 20 aktiviert daraufhin den Paketgenerator 22 zur Freigabe der benötigten Pakete zur Übertragung durch den ISP 11 über das Internet 14. Falls

(i) der Bediener die Zahlen-Internetadresse bereitgestellt hat, oder

(ii) der Bediener die Klartext-Internetadresse bereitgestellt hat, aber der Paketgenerator 22 bereits die Zahlen-Internetadresse besitzt, welche der durch den Bediener eingegebenen Klartext-Internetadresse entspricht,

kann der Paketgenerator 22 unmittelbar nach Aktivierung durch die Bedienerschnittstelle 20 die Pakete erzeugen und diese an die Netzwerkschnittstelle 21 zur Übertragung an den ISP 11 liefern.

Falls aber der Bediener die Klartext-Internetadresse der Vorrichtung 13, an welche die Pakete zu übertragen sind, eingegeben hat, und falls der Paketgenerator 22 die entsprechende Zahlen-Internetadresse davon nicht bereits besitzt, ermöglicht es der Paketgenerator 22, daß die Netzwerkadresse von dem Namen-Server 17, der in dem IP-Parameterspeicher 25 identifiziert ist, erhalten wird.

Bei diesem Vorgang wird der Paketgenerator 22 anfänglich den Namen-Server 17 kontaktieren, um zu versuchen, die geeignete Zahlen-Internetadresse von dem Namen-Server 17 zu erhalten. Bei diesem Vorgang wird die Vorrichtung 12(m) geeignete Nachrichtenpakete zur Übertragung an den Namen-Server 17 unter Verwendung der Zahlen-Internetadresse des Namen-Servers 17 erzeugen, welche durch den ISP 11 bereitgestellt wird, wenn sich die Vorrichtung 12(m) zu Beginn der Kommunikationssitzung einloggt. Jedenfalls wenn der Namen-Server 17 die Zahlen-Internetadresse für den Klartextnamen besitzt oder erhalten kann, wird der Namen-Server 17 die Zahlen-Internetadresse an die Vorrichtung 12(m) übermitteln. Die Zahlen-Internetadresse wird durch den Paketgenerator 22 über die Netzwerkschnittstelle 21 und den Paketempfänger und -prozessor 23 empfangen. Nachdem der Paketgenerator 22 die Zahlen-Internetadresse empfangen hat, kann er die notwendigen Nachrichtenpakete zur Übertragung an die Vorrichtung 13 durch die Netzwerkschnittstelle 21 und den ISP 11 erzeugen.

Wie oben ausgeführt wurde, ist in **Fig.** 1 eine der Vorrichtungen 13, welche an das Internet 14 angeschlossen sind, ein virtuelles privates Netzwerk 15, wobei das virtuelle private Netzwerk 15 eine Firewall bzw. ein Firewall-System 30, mehrere als Server 31(s) gekennzeichnete Vorrichtungen und einen Namen-Server 32 aufweist, die durch eine Übertragungsverbindung 33 miteinander verbunden sind. Die Server 31(s), die Firewall 30 und der Namen-Server 32 können als z. B. in einem LAN oder WAN verbundene Vorrichtungen untereinander Information in Form von Nachrichtenpaketen austauschen. Da die Firewall 30 mit dem Internet 14 verbunden ist und darüber Nachrichtenpakete empfangen kann, hat sie auch eine Internetadresse. Zusätzlich haben wenigstens die Server 31(s), welche über das Internet zugänglich sind, auch jeweilige Internetadressen. Dabei dient der Namen-Server 32 der Umwandlung von Klartext-Internetadressen für die Server 31(s) innerhalb des virtuellen privaten Netzwerkes 15 in die jeweiligen Zahlen-Internetadressen.

Im allgemeinen wird das virtuelle private Netzwerke 15 von einem Unternehmen, einem Regierungsamt, einer Organisation oder ähnlichem gehalten, welche möchten, daß die Server 31(s) Zugriff auf andere Vorrichtungen außerhalb des virtuellen privaten Netzwerkes 15 haben und an diese Information über das Internet 14 übertragen können, aber welche ebenfalls möchten, daß der Zugriff an die Server 31(s) durch Vorrichtungen 12(m) und andere externe Vorrichtungen über das Internet 14 in einer kontrollierten Weise begrenzt ist. Die Firewall 30 dient dazu, den Zugriff durch Vorrichtungen außerhalb des virtuellen privaten Netzwerkes 15 auf Server 31(s) innerhalb des virtuellen privaten Netzwerkes 15 zu kontrollieren. Bei diesem Vorgang stellt die Firewall 30 auch die Verbindung zum Internet 14 her und empfängt Nachrichtenpakete darüber zur Übertragung an einen Server 31(s). Falls das Nachrichtenpaket angibt, daß die Quelle des Nachrichtenpaketes einen Zugriff auf einen bestimmten Server 31(s) anfordert, und falls die Quelle für den Zugriff an den Server 31(s) authorisiert ist, sendet die Firewall 30 das Nachrichtenpaket über die Übertragungsverbindung 33 an den Server 31(s). Falls andererseits die Quelle nicht authorisiert ist, auf den Server 31(s) zuzugreifen, wird die Firewall 30 das Nachrichtenpaket nicht an den Server 31(s) übersenden, und kann anstelle ein Antwortnachrichtenpaket an die Quellenvorrichtung übermitteln, welches angibt, daß die Quelle nicht für den Zugriff an den Server 31(s) authorisiert ist. Die Firewall kann ähnlich aufgebaut sein wie die anderen Vorrichtungen **31**(s) in dem virtuellen privaten Netzwerk **15**, wobei zusätzlich eine oder mehrere Verbindungen mit dem Internet vorhanden sind, welche allgemein durch das Bezugszeichen **43** gekennzeichnet sind.

Kommunikationen zwischen Vorrichtungen außerhalb des virtuellen privaten Netzwerkes **15**, z. B. der Vorrichtung **12**(m), und einer Vorrichtung, z. B. einem Server **31**(s), innerhalb des virtuellen privaten Netzwerkes **15** kann über einen Sicherheitstunnel zwischen der Firewall **30** und der externen Vorrichtung, wie es oben beschrieben ist, erreicht werden, damit die ausgetauschten Information geheim bleiben, während diese über das Internet **14** und durch den ISP **11** übertragen werden. Ein Sicherheitstunnel zwischen der Vorrichtung **12**(m) und dem virtuellen privaten Netzwerk **15** ist in **Fig.** 1 durch logische Verbindungen dargestellt, welche durch die Bezugszeichen **40**, **42** und **44** gekennzeichnet sind; es versteht sich, daß die logischen Verbindung **42** eine der logischen Verbindungen **41** zwischen dem ISP **11** und dem Internet **14** und die logische Verbindung **44** eine der logischen Verbindungen **43** zwischen dem Internet **14** und der Firewall **30** umfaßt.

Der Aufbau eines Sicherheitstunnels kann durch eine Vorrichtung **12**(m), die extern zu dem virtuellen privaten Netzwerk **15** ist, ausgelöst werden. Bei diesem Vorgang erzeugt die Vorrichtung **12**(m) in Reaktion auf eine Aufforderung durch deren Bediener ein Nachrichtenpaket zur Übertragung durch den ISP **11** und das Internet **14** an die Firewall **30**, welches den Aufbau eines Sicherheitstunnels zwischen der Vorrichtung **12**(m) und der Firewall **30** anfordert. Das Nachrichtenpaket kann an eine bestimmte Zahlen-Internetadresse gerichtet sein, welche der Firewall **30** zugeordnet ist und welche für Sicherheitstunnelaufbauanfragen reserviert ist, und welche ferner der Vorrichtung **12**(m) bekannt ist und durch den Namen-Server **17** bereitgestellt wird. Falls die Vorrichtung **12**(m) authorisiert ist, auf einen Server **31**(s) in dem virtuellen privaten Netzwerk **15** zuzugreifen, nehmen die Vorrichtung **12**(m) als Client und die Firewall **30** einen Dialog auf, welcher den Austausch von einem oder mehreren Nachrichtenpaketen über das Internet **14** umfaßt. Während des Dialogs kann die Firewall **30** der Vorrichtung **12**(m) die Identifizierung eines Entschlüsselungsalgorithmus und einen zugehörigen Entschlüsselungsschlüssel bereitstellen, welche die Vorrichtung **12**(m) beim Entschlüsseln der verschlüsselten Abschnitte der Nachrichtenpakete zu verwenden hat, welche das virtuelle private Netzwerk an die Vorrichtung **12**(m) überträgt. Zusätzlich dazu kann die Firewall **30** der Vorrichtung **12**(m) auch die Identifizierung eines Verschlüsselungsalgorithmus und einen zugehörigen Verschlüsselungsschlüssel bereitstellen, welche die Vorrichtung **12**(m) beim Verschlüsseln der Abschnitte der Nachrichtenpakete zu verwenden hat, welche die Vorrichtung **12**(m) an das virtuelle private Netzwerk **15** überträgt und welche verschlüsselt werden sollen. Alternativ dazu kann die Vorrichtung **12**(m) die Identifizierung des Verschlüsselungsalgorithmus und des Verschlüsselungsschlüssels, welche die Vorrichtung **12**(m) verwenden wird, an die Firewall **30** während des Dialogs liefern. Die Vorrichtung **12**(m) kann in ihrem IP-Parameterspeicher **25** Informationen betreffend den Sicherheitstunnel speichern, einschließlich der Information in Verbindung mit der Identifizierung der Firewall **30** und der Identifizierungen der Verschlüsselungs- und Entschlüsselungsalgorithmen und dazugehöriger Schlüssel für Nachrichtenpakete, welche durch den Sicherheitstunnel übertragen werden.

Sodann können die Vorrichtung **12**(m) und die Firewall **30** Nachrichtenpakete über den Sicherheitstunnel übertragen. Beim Erzeugen von Nachrichtenpaketen zur Übertragung über den Sicherheitstunnel verwendet die Vorrichtung **12**(m) den Sicherheits-Paketprozessor **26**, um die Abschnitte der Nachrichtenpakete zu verschlüsseln, welche vor der Übertragung durch die Netzwerkschnittstelle **21** an den ISP **11** zur Übertragung über das Internet **14** an die Firewall **30** verschlüsselt werden sollen, und um die verschlüsselten Abschnitte der Nachrichtenpakete zu entschlüsseln, welche durch die Vorrichtung **12**(m) empfangen werden und welche verschlüsselt sind. Insbesondere nachdem der Paketgenerator **22** ein Nachrichtenpaket zur Übertragung an die Firewall **30** über den Sicherheitstunnel erzeugt hat, liefert er das Nachrichtenpaket an den Sicherheits-Paketprozessor **26**. Der Sicherheits-Paketprozessor **26** verschlüsselt daraufhin die Abschnitte des Nachrichtenpakets, welche verschlüsselt werden sollen, unter Verwendung des Verschlüsselungsalgorithmus und des Verschlüsselungsschlüssels. Nachdem die Firewall **30** ein Nachrichtenpaket von der Vorrichtung **12**(m) über den Sicherheitstunnel empfangen hat, wird sie dieses entschlüsseln und, falls der beabsichtigte Empfänger des Nachrichtenpakets eine andere Vorrichtung, z. B. ein Server **31**(s), in dem virtuellen privaten Netzwerk **15** ist, wird die Firewall **30** das Nachrichtenpaket an diese andere Vorrichtung über die Übertragungsverbindung **33** übertragen.

Wenn ein Nachrichtenpaket von einer Vorrichtung, z. B. einem Server **31**(s), in dem virtuellen privaten Netzwerk **15** an die Vorrichtung **12**(m) über den Sicherheitstunnel übertragen werden soll, empfängt die Firewall **30** ein solches Nachrichtenpaket über die Übertragungsverbindung **33** und verschlüsselt das Nachrichtenpaket zur Übertragung über das Internet **14** an den ISP **11**. Der ISP **11** sendet daraufhin das Nachrichtenpaket an die Vorrichtung **12**(m), insbesondere an deren Netzwerkschnittstelle **21**. Die Netzwerkschnittstelle **21** liefert das Nachrichtenpaket an den Sicherheits-Paketprozessor **26**, welcher die verschlüsselten Abschnitte des Nachrichtenpakets unter Verwendung des Entschlüsselungsalgorithmus und -schlüssels entschlüsselt.

Ein Problem tritt auf im Zusammenhang mit Zugriffen durch eine Vorrichtung, z. B. einer Vorrichtung **12**(m), welche extern zum virtuellen privaten Netzwerk **15** ist, und einer Vorrichtung, z. B. einem Server **31**(s), welche extern zu der Firewall ist, nämlich dann, wenn dem Namen-Server **17** keine Zahlen-Internetadressen für die Server **31**(s) und andere Vorrichtungen bereitgestellt sind, die sich innerhalb des virtuellen privaten Netzwerkes **15** befinden – mit Ausnahme der Zahlen-Internetadressen, welche der Firewall **30** zugeordnet sind. Folglich wird die Vorrichtung **12**(m) nach Eingabe der Klartext-Internetadresse durch den Bediener nicht in der Lage sein, die Zahlen-Internetadresse des Servers **31**(s) zu erhalten, wenn er auf den Namen-Server **17** zugreift.

Wenn die Vorrichtung **12**(m) und die Firewall **39** zusammenarbeiten, um einen dazwischenliegenden Sicherheitstunnel aufzubauen, liefert die Firewall **30** zur Behebung des obigen Problems an die Vorrichtung **12**(m) zusätzlich zu möglichen Identifikationen der Verschlüsselungs- und Entschlüsselungsalgorithmen und -schlüsseln, welche im Zusammenhang mit der Übertragung der Nachrichtenpakete über den Sicherheitstunnel zu verwenden sind, an die Vorrichtung **12**(m) auch die Identifizierung eines Namen-Servers, z. B. eines Namen-Servers **32**, innerhalb des virtuellen privaten Netzwerkes **15**, auf welchen die Vorrichtung **12**(m) zugreifen kann, um die geeigneten Zahlen-Internetadressen für die Klartext-Internetadressen zu erhalten, welche durch den Bediener einer Vorrichtung **12**(m) eingegeben werden. Die Identifizierung des Namen-Servers **32** wird ebenfalls in dem IP-Parameterspeicher **25** gespeichert, zusammen mit der Identifizierung des Namen-Servers **17**, welche durch den ISP **11** bereitgestellt wurde, sobald die Vorrichtung **12**(m) beim ISP **11** zu Beginn einer Kommunikationssitzung eingeloggt wurde. Wenn daher die Vorrichtung **12**(m) ein Nachrichtenpaket an eine Vorrichtung, z. B. einen Server **31**(s), in dem virtuellen privaten Netzwerk **15** unter Verwendung einer Klartext-Internetadresse übertragen möchte, welche z. B. durch einen Bediener bereitgestellt bzw. eingegeben wurde, greift die Vorrichtung **12**(m) zu Beginn auf den Namen-Server **17** zu, wie es oben beschrieben wurde, um zu versuchen, die zu der Klartext-Internetadresse zugehörige Zahlen-Internetadresse zu erhalten. Da der Namen-Server **17** außerhalb des virtuellen privaten Netzwerkes **15** ist und die durch die Vorrichtung **12**(m) angeforderten Information nicht besitzt, sendet er ein entsprechend lautendes Antwortnachrichtenpaket. Die Vorrichtung **12**(m) wird sodann ein Anfragenachrichtenpaket zur Übertragung an den Namen-Server **32** durch die Firewall **30** und über den Sicherheitstunnel erzeugen. Falls der Namen-Server **32** eine Zahlen-Internetadresse besitzt, welche zu der Klartext-Internetadresse in dem Anfragenachrichtenpaket gehört, welches durch die Vorrichtung **12**(m) geliefert wird, stellt er die Zahlen-Internetadresse in einer Weise bereit, welche im allgemeinen derjenigen ähnlich ist, welche oben im Zusammenhang mit dem Namen-Server **17** beschrieben wurde mit der Ausnahme, daß die Zahlen-Internetadresse durch den Namen-Server **32** in einem an die Firewall **30** gerichteten Nachrichtenpaket geliefert wird, und die Firewall **30** sodann das Nachrichtenpaket über den Sicherheitstunnel an die Vorrichtung **12**(m) übermittelt. Es versteht sich, daß sich in dem Nachrichtenpaket, welches durch die Firewall **30** übertragen wird, die Zahlen-Internetadresse in dem Nachrichtenpaket im Datenabschnitt des Nachrichtenpakets befindet, welches über den Sicherheitstunnel übertragen wird und entsprechend verschlüsselt sein wird. Das Nachrichtenpaket wird durch die Vorrichtung **12**(m) in einer ähnlichen Weise verarbeitet, wie sie oben im Zusammenhang mit anderen Nachrichtenpaketen beschrieben wurde, welche durch die Vorrichtung **12**(m) über den Sicherheitstunnel empfangen werden. Das heißt, daß das Nachrichtenpaket durch den Sicherheits-Paketprozessor **26** vor dem Übermitteln an den Paketempfänger und -prozessor **23** zur Verarbeitung entschlüsselt wird. Die Zahlen-Internetadresse für den Server **31**(s) kann in einem Cache in einer Zugriffskontrolliste (ACL) in dem IP-Parameterspeicher **25** gespeichert werden, zusammen mit der Zuordnungsinformation bezüglich der zugehörigen Klartext-Internetadresse, einer Angabe, daß der Server **31**(s), der dieser Klartext-Internetadresse zugeordnet ist, über die Firewall **30** des virtuellen privaten Netzwerkes **15** zugänglich ist, und die Identifizierungen der Verschlüsselungs- und Entschlüsselungsalgorithmen und -schlüssel, welche für eine Verschlüsselung und Entschlüsselung der geeigneten Abschnitte der Nachrichtenpakete zu verwenden sind, welche an den Server **31**(s) übertragen und von diesem erhalten werden.

Es versteht sich, daß in Reaktion auf ein Nachrichtenpaket von der Vorrichtung **12**(m), welches beim Namen-Server **32** die Bereitstellung einer Zahlen-Internetadresse für eine durch die Vorrichtung **12**(m) angegebene Klartext-Internetadresse anfordert, falls der Namen-Server **32** keine Zuordnungsinformation zwischen der Klartext-Internetadresse und einer Zahlen-Internetadresse besitzt, der Namen-Server **32** ein Antwortnachrichtenpaket, das entsprechend lautet, übertragen kann. Falls die Vorrichtung **12**(m) eine Identifizierung von anderen Namen-Servern besitzt, welche z. B. mit anderen virtuellen privaten Netzwerken (nicht gezeigt) verbunden sein können und zu welchen die Vorrichtung **12**(m) Zugriff hat, dann kann die Vorrichtung **12**(m) versuchen, auf die anderen Namen-Server in einer ähnlichen Weise, wie es oben beschrieben ist, zuzugreifen. Falls die Vorrichtung **12**(m) nicht in der Lage ist, eine Zahlen-Internetadresse, welche der Klartext-Internetadresse zugeordnet ist, von irgendeinem der Namen-Server zu erhalten, zu welchem sie Zugriff hat und welche im allgemeinen im IP-Parameterspeicher **25** der Vorrichtung **12**(m) identifiziert sind, wird sie allgemein nicht in der Lage sein, auf eine Vorrichtung mit der vorgegebenen Klartext-Internetadresse zuzugreifen und wird den Bediener oder ein Programm, welche den Zugriff angefordert haben, dementsprechend unterrichten.

Mit diesem Hintergrund werden nun Operationen, welche durch die Vorrichtung **12**(m) und das virtuelle private Netzwerk **15** in Verbindung mit der vorliegenden Erfindung durchgeführt werden, im Detail beschrieben. Im allgemeinen laufen die Operationen in zwei Phasen ab. In einer ersten Phase arbeiten die Vorrichtung **12**(m) und das virtuelle private Netzwerk **15** zusammen, um einen Sicherheitstunnel durch das Internet **14** aufzubauen. In dieser ersten Phase liefert das virtuelle private Netzwerk **15**, insbesondere die Firewall **30**, die Identifizierung eines Namen-Servers **32**, und es kann auch die den Verschlüsselungs- und Entschlüsselungsalgorithmus und -schlüssel betreffende Information bereitstellen, wie es oben beschrieben wurde. In der zweiten Phase, nachdem der Sicherheitstunnel eingerichtet wurde, kann die Vorrichtung **12**(m) die während der ersten Phase gelieferten Information im Zusammenhang mit der Erzeugung und Übertragung von Nachrichtenpaketen an einen oder mehrere Server **31**(s) in dem virtuellen privaten Netzwerk **15** und bei dem notwendigen Umwandlungsvorgang der Klartext-Internetadressen zu Zahlen-Internetadressen aus dem Namen-Server **32**, welcher durch die Firewall **30** während der ersten Phase identifiziert wurde, verwenden.

Folglich erzeugt die Vorrichtung **12**(m) in der ersten (Sicherheitstunnelaufbau)phase zu Beginn ein Nachrichtenpaket zur Übertragung an die Firewall **30**, welches einen Aufbau eines Sicherheitstunnels anfordert. Das Nachrichtenpaket enthält eine Zahlen-Internetadresse für die Firewall, (welche durch den Bediener der Vorrichtung oder ein Programm bereitgestellt werden kann, welches durch die Vorrichtung **12**(m) verarbeitet wird, oder durch den Namen-Server **17** bereitgestellt werden kann, nachdem eine Klartext-Internetadresse durch den Bediener oder ein Programm bereitgestellt wurde), und welche insbesondere dazu dient, die Firewall **30** zu veranlassen, mit der Vorrichtung **12**(m) einen Sicherheitstunnel aufzubauen. Falls die Firewall **30** die Anfrage bezüglich des Sicherheitstunnelaufbaus akzeptiert und falls die Firewall **30** die Verschlüsselungs- und Entschlüsselungsalgorithmen und -schlüssel bereitstellt, so wie es oben angegeben wurde, erzeugt die Firewall **30** ein Antwortnachrichtenpaket zur Übertragung an die Vorrichtung **12**(m), welches die Verschlüsselungs- und Entschlüsselungsalgorithmen und -schlüssel identifiziert. Wie oben beschrieben, wird dieses Antwortnachrichtenpaket nicht verschlüsselt. Wenn die Vorrichtung **12**(m) die Antwort empfängt, werden die Identifizierungen der Verschlüsselungs- und Entschlüsselungsalgorithmen und -schlüssel in dem IP-Parameterspeicher **25** gespeichert.

Zu einem späteren Zeitpunkt in der ersten Phase erzeugt die Firewall **30** auch ein Nachrichtenpaket zur Übertragung an die Vorrichtung **12**(m), welches die Zahlen-Internetadresse des Namen-Servers **32** enthält. Bei diesem Nachrichtenpaket wird der Abschnitt des Nachrichtenpakets, welcher die Zahlen-Internetadresse des Namen-Servers **32** enthält, unter Verwendung eines Verschlüsselungsalgorithmus und Verschlüsselungsschlüssels verschlüsselt, und dies kann unter Verwendung des Entschlüsselungsalgorithmus und -schlüssels, die durch das zuvor beschriebene Antwortnachrichtenpaket geliefert wurden, wieder entschlüsselt werden. Diese Nachricht hat im allgemeinen die folgende Struktur:

"<IIA(FW),IIA(DEV12(m)><SEC_TUN>
<ENCR<<IIA(FW),IIA(DEV_12(m)><(DNS_ADRS:IIA(-NS_2>>>"

wobei

(i) "IIA(FW)" die Quellenadresse darstellt, d. h. eine Zahlen-Internetadresse der Firewall **30**,
(ii) "IIA(DEV_12(m))" die Zieladresse darstellt, d. h. die Zahlen-Internetadresse der Vorrichtung **12** (m),
(iii) "DNS_ADRS:IIA(NS)" angibt, daß "IIA(NS_32)" die Zahlen-Internetadresse des Namen-Servers **32** darstellt, für dessen Benutzung die Vorrichtung **12**(m) authorisiert ist, und
(iv) "ENCR<. . . >" bedeutet, daß die Information, zwischen den Klammern "<" und ">" verschlüsselt ist.

Der Anfangsabschnitt der Nachricht "IIA(FW),IIA(DEV_12(m))>" bildet wenigstens einen Teil des Kopfabschnitts der Nachricht, und "<ENCR<<IIA(FW),IIA(DEV_12(m))><IIA(NS>>>" stellt wenigstens einen Teil des Datenabschnitts der Nachricht dar. "<SEC_TUN>" stellt einen Hinweis in dem Kopfabschnitt dar, welcher angibt, daß die Nachricht über den Sicherheitstunnel übertragen wird, wodurch auch angezeigt wird, daß der Datenabschnitt der Nachricht verschlüsselte Information enthält.

Nachdem die Vorrichtung **12**(m) die Nachricht von der Firewall **30** empfängt, wie es oben beschrieben wurde, und weil das Nachrichtenpaket den <SEC_TUN> Hinweis enthält, überträgt deren Netzwerkschnittstelle **21** den verschlüsselten Abschnitt "<ENCR<<IIA(FW),IIA(DEV_12(m)><DNS_ADRS:IIA(-NS_32)>>>" an den Sicherheits-Paketprozessor **26** zur Verarbeitung. Der Sicherheits-Paketprozessor **26** entschlüsselt den verschlüsselten Abschnitt, bestimmt weiter, daß der Abschnitt "IIA(NS_32)" die Zahlen-Internetadresse des Namen-Servers darstellt, insbesondere des Namen-Servers **32**, für dessen Benutzung die Vorrichtung **12**(m) authorisiert ist, und speichert diese Adresse in dem IP-Parameterspeicher **25** zusammen mit einer Angabe, daß die dorthin gerichteten Nachrichtenpakete zu der Firewall **30** zu übertragen sind, und daß die Daten in den Nachrichtenpaketen unter Verwendung des Verschlüsselungsalgorithmus und -schlüssels, die davor durch die Firewall **30** übermittelt wurden, zu verschlüsseln sind. Es versteht sich, daß aufgrund der Tatsache, daß die Zahlen-Internetadresse des Namen-Servers **32** von der Firewall an die Vorrichtung **12**(m) in verschlüsselter Form übertragen wird, diese vertraulich bleibt, selbst wenn das Paket durch einen Dritten abgefangen wird.

In Abhängigkeit des speziellen Protokolls, welches für den Aufbau des Sicherheitstunnels verwendet wird, können die Firewall **30** und die Vorrichtung **12**(m) auch Nachrichtenpakete austauschen, welche andere Information enthalten als die oben beschriebenen.

Wie oben erwähnt wurde, kann die Vorrichtung **12**(m) in der zweiten Phase nach der Einrichtung des Sicherheitstunnels die Information, welche während der ersten Phase bereitgestellt wurde, im Zusammenhang mit dem Erzeugen und Übertragen von Nachrichtenpaketen zu einem oder mehreren der Server **31**(s) in dem virtuellen privaten Netzwerk **15** nutzen. Falls bei diesen Operationen der Bediener einer Vorrichtung **12**(m) oder ein Programm, welches durch eine Vorrichtung **12**(m) verarbeitet wird, möchte, daß die Vorrichtung **12**(m) ein Nachrichtenpaket an einen Server **31**(s) in dem virtuellen privaten Netzwerk **15** überträgt, und falls der Bediener durch die Bedienerschnittstelle **20** oder das Programm eine Klartext-Internetadresse bereitstellt, wird zunächst die Vorrichtung **12**(m), insbesondere der Paketgenerator **22**, bestimmen, ob der IP-Parameterspeicher **25** dort in einem Cache eine Zahlen-Internetadresse gespeichert hat, welche zu der Klartext-Internetadresse gehört. Falls dies nicht der Fall ist, erzeugt der Paketgenerator **22** ein Anfragenachrichtenpaket zur Übertragung an den Namen-Server **17**, um von diesem die zu der Klartext-Internetadresse gehörige Zahlen-Internetadresse anzufordern. Falls der Namen-Server **17** eine zu der Klartext-Internetadresse gehörige Zahlen-Internetadresse besitzt, wird dieser die Zahlen-Internetadresse an die Vorrichtung **12**(m) liefern. Es versteht sich, daß dies nur erfolgen kann, wenn die Klartext-Internetadresse im Anfragenachrichtenpaket sowohl einer Vorrichtung **13** außerhalb des virtuellen privaten Netzwerkes **15** als auch einem Server **32**(s) in dem virtuellen privaten Netzwerk **15** zugeordnet wurde. Danach kann die Vorrichtung **12**(m) die Zahlen-Internetadresse verwenden, um Nachrichtenpakete zur Übertragung über das Internet zu erzeugen, wie es oben beschrieben wurde.

Falls andererseits angenommen wird, daß der Namen-Server **17** keine der Klartext-Internetadresse zugeordnete Zahlen-Internetadresse besitzt, wird der Namen-Server **17** ein entsprechend lautendes Antwortnachrichtenpaket an die Vorrichtung **12**(m) übermitteln. Sodann erzeugt der Paketgenerator **22** der Vorrichtung **12**(m) ein Anfragenachrichtenpaket zur Übertragung au den nächsten Namen-Server, der in ihrem IP-Parameterspeicher **25** identifiziert ist, um von diesem Namen-Server die der Klartext-Internetadresse zugeordnete Zahlen-Internetadresse anzufordern. Falls dieser nächste Namen-Server der Namen-Server **32** ist, liefert der Paketgenerator **22** das Nachrichtenpaket an den Sicherheits-Paketprozessor **26** zur weiteren Verarbeitung. Der Sicherheits-Paketprozessor **26** erzeugt daraufhin ein Anfragenachrichtenpaket zur Übertragung über den Sicherheitstunnel an die Firewall **30**. Diese Nachricht hat im allgemeinen folgende Struktur:

"<IIA(DEV_12(m)),IIA(FW)><SEC_TUN>
<ENCR<<IIA(DEV_12(m)),IIA(NS_32))><IIA_REQ>>>-"

wobei

(i) "IIA(DEV_12(m))" die Quellenadresse darstellt, d. h. die Zahlen-Internetadresse der Vorrichtung **12**(m),
(ii) "IIA(FW)" die Zieladresse darstellt, d. h. die Zahlen-Internetadresse der Firewall **30**,
(iii) "IIA(NS_32)" die Adresse des Namen-Servers **32** darstellt,
(iv) "<<IIA(DEV_12(m)),IIA(NS_32))><IIA_REQ>->>" das Anfragenachrichtenpaket darstellt, welches durch den Paketgenerator **22** erzeugt wird, wobei "<IIA(DEV_12(m)),IIA(NS_32)>" den Kopfabschnitt des Anfragenachrichtenpakets und "<IIA_REQ>" den Datenabschnitt des Anfragenachrichtenpakets darstellt,
(v) "ENCR<. . . >" angibt, daß die Information zwischen den Klammern "<" und ">" verschlüsselt ist, und
(vi) "<SEC_TUN>" einen Hinweis in dem Kopfabschnitt des Nachrichtenpakets darstellt, welches durch den Sicherheitspaketgenerator **26** erzeugt wird und angibt, daß die Nachricht über den Sicherheitstunnel übertragen wird, wobei hierdurch angegeben wird, daß der Datenabschnitt der Nachricht verschlüsselte Information enthält.

Wenn die Firewall **30** das durch den Sicherheitspaketgenerator **26** erzeugte Anfragenachrichtenpaket empfängt, wird diese den verschlüsselten Abschnitt des Nachrichtenpakets entschlüsseln, um "<<IIA(DEV_12(m)),IIA(NS_32))><IIA_REQ>>" zu erhalten. Dies stellt das Anfragenachrichtenpaket dar, welches durch den Paketgenerator **22** erzeugt wird. Nachdem das Anfragenachrichtenpaket erhalten wurde, überträgt die Firewall **30** dieses über die Übertragungsverbindung **33** an den Namen-Server **32**. In Abhängigkeit von dem Protokoll zur Übertragung von Nachrichtenpaketen über die Übertragungsverbindung **33** kann es bei diesem Prozeß für die Firewall **30** notwendig sein, das Anfragenachrichtenpaket zu modifizieren, damit es dem Protokoll der Übertragungsverbindung **33** entspricht.

Nachdem der Namen-Server **32** das Anfragenachrichtenpaket erhalten hat, wird dieser das Anfragenachrichtenpaket verarbeiten, um zu bestimmen, ob er eine der Klartext-Internetadresse, welche in dem Anfragenachrichtenpaket gesendet wird, zugeordnete Zahlen-Internetadresse besitzt. Falls der Namen-Server feststellt, daß er eine solche Zahlen-Internetadresse aufweist, wird dieser ein Antwortnachrichtenpaket zur Übertragung an die Firewall erzeugen, welches die Zahlen-Internetadresse enthält. Im allgemeinen hat das Antwortnachrichtenpaket die folgende Struktur:

"<<IIA(NS_32),IIA(DEV_12(m)><IIA_RESP>>"

wobei

(i) "IIA(NS_32)" die Quellenadresse darstellt, d. h. die Zahlen-Internetadresse des Namen-Servers **32**,
(ii) "IIA(DEV_12(m))" die Zieladresse darstellt, d. h. die Zahlen-Internetadresse der Vorrichtung **12**(m), und
(iii) "IIA_RESP" die Zahlen-Internetadresse darstellt, welche der Klartext-Internetadresse zugeordnet ist.

Nachdem die Firewall **30** das Antwortnachrichtenpaket empfangen hat, und weil die Kommunikation mit der Vorrichtung **12**(m) über den dazwischenliegenden Sicherheitstunnel stattfindet, verschlüsselt die Firewall **30** das von dem Namen-Server **32** empfangene Antwortnachrichtenpaket und erzeugt ein Nachrichtenpaket zur Übertragung an die Vorrichtung **12**(m), welches das verschlüsselte Antwortnachrichtenpaket enthält. Im allgemeinen hat das durch die Firewall **30** erzeugte Nachrichtenpaket die folgende Struktur:

"<IIA(FW),IIA(DEV12(m)><SEC_TUN)>
<ENCR<<IIA(NS_32),IIA(DEV_12(m))><IIA_RESP>>->"

wobei

(i) "IIA(FW)" die Quellenadresse darstellt, d. h. die Zahlen-Internetadresse der Firewall **30**,
(ii) "IIA(DEV_12(m))" die Zieladresse darstellt, d. h. die Zahlen-Internetadresse der Vorrichtung **12**(m),
(iii) "SEC_TUN" einen Hinweis in dem Kopfabschnitt des Nachrichtenpakets darstellt, welches durch den Sicherheitspaketgenerator **26** erzeugt wird, und angibt, daß die Nachricht über den Sicherheitstunnel übertragen wird, und wobei auch angegeben wird, daß der Datenabschnitt der Nachricht verschlüsselte Information enthält,
(iv) "ENCR<. . . .>" angibt, daß die Information zwischen den Klammern "<" und ">" (was dem von dem Namen-Server **32** empfangenen Antwortnachrichtenpaket entspricht) verschlüsselt ist.

Zusätzlich kann es je nach dem Protokoll zur Übertragung von Nachrichtenpaketen über die Übertragungsverbindung **33** für die Firewall **30** notwendig sein, das Nachrichtenpaket zu bearbeiten und/oder zu modifizieren, damit dieses dem Protokoll des Internets **14** entspricht.

Wenn die Vorrichtung **12**(m) das Nachrichtenpaket von der Firewall **30** empfängt, wird das Nachrichtenpaket an den Sicherheits-Paketprozessor **26** geliefert. Der Sicherheitspaketprozessor **26** entschlüsselt daraufhin den verschlüsselten Abschnitt des Nachrichtenpakets, um die der Klartext-Internetadresse zugeordnete Zahlen-Internetadresse zu erhalten und lädt diese Information in den IP-Parameterspeicher **25**. Danach kann die Vorrichtung diese Zahlen-Internetadresse beim Erzeugen von Nachrichtenpaketen zur Übertragung an den Server **31**(s) verwenden, welcher zu der Klartext-Internetadresse gehört.

Es versteht sich, daß, falls der Namen-Server **32** keine Zahlen-Internetadresse besitzt, welche der durch die Vorrichtung **12**(m) in dem Anfragenachrichtenpaket gelieferte Klartext-Internetadresse zugeordnet ist, dies der Namen-Server **32** in dem durch ihn erzeugten Antwortnachrichtenpaket entsprechend anzeigen. Die Firewall **30** erzeugt dann in Reaktion auf das durch den Namen-Server **32** gelieferte Antwortnachrichtenpaket auch ein Nachrichtenpaket zur Übertragung an die Vorrichtung **12**(m), welches einen verschlüsselten Abschnitt enthält, der das Antwortnachrichtenpaket umfaßt, das durch den Namen-Server **32** erzeugt wurde. Nachdem die Vorrichtung **12**(m) das Nachrichtenpaket empfangen hat, wird der verschlüsselte Abschnitt durch den Sicherheitspaketprozessor **26** entschlüsselt, welcher daraufhin den Paketgenerator **22** darüber informiert, daß der Namen-Server **32** keine der Klartext-Internetadresse zugeordnete Zahlen-Internetadresse besitzt. Falls der IP-Parameterspeicher **25** die Identifizierung eines anderen Namen-Servers enthält, erzeugt sodann der Paketgenerator **22** der Vorrichtung **12**(m) ein Anfragenachrichtenpaket zur Übertragung an den nächsten Namen-Server, der in deren IP-Parameterspeicher **25** identifiziert ist, um von diesem Namen-Server die Zahlen-Internetadresse anzufordern, welche der Klartext-Internetadresse zugeordnet ist. Falls andererseits der IP-Parameterspeicher **25** keine Identifizierung eines anderen Namen-Servers enthält, kann der Paketgenerator **22** die Bedienerschnittstelle **20** oder ein Programm darüber informieren, daß er nicht in der Lage ist, ein Nachrichtenpaket zur Übertragung an eine Vorrichtung zu erzeugen, welche der Klartext-Internetadresse zugeordnet ist, welche durch die Bedienerschnittstelle **20** oder ein Programm eingegeben bzw. bereitgestellt wurde.

Die Erfindung liefert eine Anzahl von Vorteilen. Insbesondere schafft die Erfindung ein System zum Vereinfachen der Kommunikation zwischen Vorrichtungen, welche mit einem öffentlichen Netzwerk verbunden sind, z. B. mit dem Internet **14**, und Vorrichtungen, welche mit privaten Netzwerken verbunden sind, z. B. mit dem virtuellen privaten Netzwerk **15**, indem die Umwandlung von Klartextadressen in Netzwerkadressen durch einen Namen-Server, der bevorzugt über einen Sicherheitstunnel mit den privaten Netzwerken verbunden ist, ermöglicht wird.

Es versteht sich, daß eine Vielzahl von Modifikationen an der im Zusammenhang mit **Fig.** 1 beschriebenen Anordnung durchgeführt werden können. Obwohl das Netzwerk **10** so beschrieben wurde, daß die Identifizierung der Verschlüsselungs- und Entschlüsselungsalgorithmen und -schlüssel durch die Vorrichtung **12**(m) und die Firewall **30** während des Dialogs, währenddessen der Sicherheitstunnel eingerichtet wird, ausgetauscht wird, versteht es sich, daß beispielsweise Information durch die Vorrichtung **12**(m) und die Firewall **30** getrennt von dem Aufbau eines solchen Sicherheitstunnels bereitgestellt werden können.

Obwohl die Erfindung im Zusammenhang mit dem Internet beschrieben wurde, versteht es sich ferner, daß die Erfindung in Verbindung mit jedem, insbesondere globalen, Netzwerk verwendet werden kann. Obwohl die Erfindung im Zusammenhang mit einem Netzwerk beschrieben wurde, welches ein System von Klartext-Netzwerkadressen bereitstellt, versteht es sich ferner, daß die Erfindung nicht darauf beschränkt ist sondern in Verbindung mit jedem Netzwerk verwendet werden kann, welches irgendeine Form einer – den systemeigenen Netzwerkadressen übergeordnete – Sekundär-Netzwerkadresseneinrichtung oder vergleichbare nicht-formeller Netzwerkadresseneinrichtung vorsieht.

Es versteht sich ferner, daß ein erfindungsgemäßes System als ganzes oder in Teilen aus speziell hierfür geeigneter Hardware oder einem allgemein geeigneten Computersystem oder jeder Kombination davon aufgebaut werden kann, wobei jeder Abschnitt davon durch ein geeignetes Programm gesteuert werden kann. Jedes Programm kann als ganzes oder in Teilen einen Teil des Systems umfassen oder auf dem System in einer konventionellen Weise gespeichert sein, oder es kann als ganzes oder in Teilen in das System über ein Netzwerk oder andere Mechanismen zur Übertragung von Information in einer konventionellen Weise bereitgestellt werden. Zusätzlich versteht es sich, daß das System betrieben und/oder auf andere Art und Weise mittels Information gesteuert werden kann, welche durch einen Bediener mittels Bedienereingabeelementen (nicht gezeigt) bereitgestellt wird, welche direkt an das System angeschlossen sein können oder welche die Information über ein Netzwerk oder ändere Mechanismen zur Übertragung von Information in einer konventionellen Weise übertragen können.

Die vorstehende Beschreibung hat sich auf ein spezifisches Ausführungsbeispiel der Erfindung bezogen. Es versteht sich jedoch, daß verschiedene Variationen und Modifikationen der Erfindung gemacht werden können, bei welchen einige oder alle der Vorteile der Erfindung erreicht werden. Diese und andere Variationen und Modifikationen fallen in den Schutzbereich der vorliegenden Erfindung, der durch die nachfolgenden Ansprüche bestimmt ist.

Patentansprüche

1. System umfassend ein virtuelles privates Netzwerk (**15**) und eine externe Vorrichtung (12 (m)), welche über ein digitales Netzwerk (**14**) kommunizieren, wobei:
das virtuelle private Netzwerk (**15**) eine Firewall (**30**), wenigstens eine interne Vorrichtung (**31**(s)) und einen Namen-Server (**32**) aufweist, welche jeweils eine Netzwerkadresse besitzen, wobei die interne Vorrichtung (**31**(s)) auch eine Sekundäradresse besitzt und der Namen-Server (**32**) derart konfiguriert ist, daß er eine Zuordnung zwischen der Sekundäradresse und der Netzwerkadresse bereitstellt,
die Firewall (**30**) derart konfiguriert ist, daß sie der externen Vorrichtung (**12**(m)) in Reaktion auf deren Anfrage zum Aufbau einer Verbindung zur Firewall (**30**) die Netzwerkadresse des Namen-Servers (**32**) liefert, und
die externe Vorrichtung (**12**(m)) derart konfiguriert ist, daß sie in Reaktion auf eine Anfrage zum Zugriff auf die interne Vorrichtung (**31**(s)), welche die Sekundäradresse der internen Vorrichtung (**31**(s)) enthält, eine Netzwerkadressen-Anfragenachricht zur Übertragung über die Verbindung an die Firewall (**30**) erzeugt, welche eine Auflösung der der Sekundäradresse zugeordneten Netzwerkadresse anfordert, wobei die Firewall (**30**) derart konfiguriert ist, daß sie die Adressenauflösungsanfrage an den Namen-Server (**32**) übermittelt, der Namen-Server (**32**) derart konfiguriert ist, daß er die der Sekundäradresse zugeordnete Netzwerkadresse bereitstellt, und die Firewall (**30**) daraufhin die Netzwerkadresse in einer Netzwerkadressen-Antwortnachricht zur Übertragung über die Verbindung an die externe Vorrichtung (**12**(m)) bereitstellt.

2. System nach Anspruch 1, bei welchem die externe Vorrichtung (**12**(m)) derart konfiguriert ist, daß sie die in der Netzwerkadressen-Antwortnachricht bereitgestellte Netzwerkadresse beim Erzeugen von wenigstens einer Nachricht zur Übertragung an die interne Vorrichtung (**31**(s)) verwendet.

3. System nach Anspruch 1 oder 2, bei welchem die externe Vorrichtung (**12**(m)) derart konfiguriert ist, daß sie mit dem Netzwerk (**14**) durch einen Netzwerk-Service-Provider (**11**) verbunden wird.

4. System nach Anspruch 3, bei welchem die externe Vorrichtung (**12**(m)) derart konfiguriert ist, daß sie eine Kommunikationssitzung mit dem Netzwerk-Service-Provider (**11**) aufbaut, wobei der Netzwerk-Service-Provider (**11**) der externen Vorrichtung (**12**(m)) die Identifizierung eines weiteren Namen-Servers übermittelt, wobei der weitere Namen-Server derart konfiguriert ist, daß er eine Zuordnung zwischen einer Sekundäradresse und einer Netzwerkadresse für wenigstens eine Vorrichtung bereitstellt.

5. System nach einem der vorstehenden Ansprüche, bei welchem die externe Vorrichtung (**12**(m)) derart konfiguriert ist, daß sie eine Liste von Namen-Servern erhält, welche der externen Vorrichtung (**12**(m)) identifiziert wurden, und die externe Vorrichtung (**12**(m)) die Namen-Server in der Liste nacheinander in Reaktion auf eine Anfrage zum Zugriff auf eine andere Vorrichtung abfragt, wobei die Anfrage eine Sekundäradresse der anderen Vorrichtung enthält, solange bis die externe Vorrichtung (**12**(m)) eine Netzwerkadresse empfängt, wobei die externe Vorrichtung (**12**(m)) in jedem Abfragevorgang eine Netzwerkadressen-Anfragesnachricht zur Übertragung über das Netzwerk (**14**) erzeugt, welche durch einen der Namen-Server in der Liste zu beantworten ist, und von diesem eine Netzwerkadressen-Antwortnachricht empfängt.

6. System nach einem der vorstehenden Ansprüche, bei welchem die Verbindung zwischen der externen Vorrichtung (**12**(m)) und der Firewall (**30**) ein Sicherheitstunnel ist, in welchem wenigstens ein der zwischen der externen Vorrichtung (**12**(m)) und der Firewall (**30**) übertragenen Nachrichten verschlüsselt ist.

7. Verfahren zum Betreiben eines Systems umfassend ein virtuelles privates Netzwerk (**15**) und eine externe Vorrichtung (**12**(m)), welche durch ein digitales Netzwerk (**14**) miteinander verbunden sind, wobei das virtuelle private Netzwerk (**15**) eine Firewall (**30**), wenigstens eine interne Vorrichtung (**31**(s)) und einen Namen-Server (**32**) aufweist, welche jeweils eine Netzwerkadresse besitzen, wobei die interne Vorrichtung (**31**(s)) auch eine Sekundäradresse besitzt, und der Namen-Server (**32**) derart konfiguriert ist, daß er eine Zuordnung zwischen der Sekundäradresse und der Netzwerkadresse bereitstellt, wobei:
A. in Reaktion auf eine Anfrage der externen Vorrichtung (**12**(m)) zum Aufbau einer Verbindung zur Firewall (**30**) die Firewall (**30**) der externen Vorrichtung (**12**(m)) die Netzwerkadresse des

Namen-Servers (**32**) übermittelt; und

B. (i) in Reaktion auf eine Anfrage zum Zugriff auf die interne Vorrichtung (**31**(s)), welche die Sekundäradresse der internen Vorrichtung (**31**(s)) enthält, die externe Vorrichtung (**12**(m)) eine Netzwerkadressen-Anfragenachricht zur Übertragung über die Verbindung an die Firewall (**30**) erzeugt, welche eine Auflösung der Netzwerkadresse, welche der Sekundäradresse zugeordnet ist, anfordert,

(ii) die Firewall (**30**) die Adressenauflösungsanfrage an den Namen-Server (**32**) übermittelt, (iii) der Namen-Server (**32**) die der Sekundäradresse zugeordnete Netzwerkadresse bereitstellt, und

(iv) die Firewall (**30**) die Netzwerkadresse in einer Netzwerkadressen-Antwortnachricht zur Übertragung über die Verbindung an die externe Vorrichtung (**12**(m)) bereitstellt.

8. Verfahren nach Anspruch 7, bei welchem die externe Vorrichtung (**12**((m) ferner die in der Netzwerkadressen-Antwortnachricht bereitgestellte Netzwerkadresse beim Erzeugen von wenigstens einer Nachricht zur Übertragung an die interne Vorrichtung (**31**(s)) verwendet.

9. Verfahren nach Anspruch 7 oder 8, bei welchem die externe Vorrichtung (**12**(m)) mit dem Netzwerk (**14**) durch einen Netzwerk-Service-Provider (**11**) verbunden werden kann.

10. Verfahren nach Anspruch 9, bei welchem die externe Vorrichtung (**12**(m)) eine Kommunikationssitzung mit dem Netzwerk-Service-Provider (**11**) aufbaut, wobei der Netzwerk-Service-Provider (**11**) der externen Vorrichtung (**12**(m)) die Identifizierung eines weiteren Namen-Servers übermittelt, wobei der weitere Namen-Server eine Zuordnung zwischen einer Sekundäradresse und einer Netzwerkadresse für wenigstens eine Vorrichtung bereitstellt.

11. Verfahren nach einem der Ansprüche 7 bis 10, bei welchem die externe Vorrichtung (**12**(m)) eine Liste von Namen-Servern erhält, welche der externen Vorrichtung (**12**(m)) identifiziert wurden, und die externe Vorrichtung (**12**(m)) die Namen-Server in der Liste nacheinander in Reaktion auf eine Anfrage zum Zugriff auf eine andere Vorrichtung abfragt, wobei die Anfrage eine Sekundäradresse der anderen Vorrichtung enthält, solange bis die externe Vorrichtung (**12**(m)) eine Netzwerkadresse empfängt, wobei die externe Vorrichtung (**12**(m)) in jedem Abfragevorgang eine Netzwerkadressen-Anfragenachricht zur Übertragung über das Netzwerk (**14**) erzeugt, welche durch einen der Namen-Server in der Liste zu beantworten ist, und von diesem eine Netzwerkadressen-Antwortnachricht empfängt.

12. Verfahren nach einem der Ansprüche 7 bis 11, bei welchem die Verbindung zwischen der externen Vorrichtung (**12**(m)) und der Firewall (**30**) ein Sicherheitstunnel ist, in welchem wenigstens ein Abschnitt der zwischen der externen Vorrichtung (**12**(m)) und der Firewall (**30**) übertragenen Nachrichten verschlüsselt ist.

13. Computerprogramm-Produkt zur gemeinsamen Verwendung mit einem virtuellen privaten Netzwerk (**15**) und einer externen Vorrichtung (**12**(m)), welche durch ein digitales Netzwerk (**14**) miteinander verbunden sind, wobei das virtuelle private Netzwerk eine Firewall (**30**), wenigstens eine interne Vorrichtung (**31**(s)) und einen Namen-Server (**32**) aufweist, welche jeweils eine Netzwerkadresse besitzen, wobei die interne Vorrichtung (**31**(s)) auch eine Sekundäradresse besitzt, und der Namen-Server (**32**) derart konfiguriert ist, daß er eine Zuordnung zwischen der Sekundäradresse und der Netzwerkadresse bereitstellt, wobei das Computerprogrammprodukt ein maschinenlesbares Medium mit folgenden Codes aufweist:

A. ein Namen-Server-Identifizierungscodemodul, welches veranlaßt, daß die Firewall (**30**) der externen Vorrichtung (**12**(m)) in Reaktion auf deren Anfrage zum Aufbau einer Verbindung zur Firewall (**30**) die Netzwerkadresse des Namen-Servers (**32**) übermittelt,

B. ein Codemodul zur Erzeugung einer Netzwerkadressen-Anfragenachricht, welches veranlaßt, daß die externe Vorrichtung (**12**(m)) in Reaktion auf eine Anfrage zum Zugriff auf die interne Vorrichtung (**31**(s)), welche die Sekundäradresse der internen Vorrichtung (**31**(s)) enthält, eine Netzwerkadressen-Anfragenachricht zur Übertragung über die Verbindung an die Firewall (**30**) erzeugt, welche die Auflösung der der Sekundäradresse zugeordneten Netzwerkadresse anfordert,

C. ein Modul zur Übermittlung einer Adressenauflösungsanfrage, welches veranlaßt, daß die Firewall (**30**) die Adressenauflösungsanfrage an den Namen-Server (**32**) übermittelt,

D. ein Namen-Server-Steuerungsmodul, welches veranlaßt, daß der Namen-Server (**32**) die der Sekundäradresse zugeordnete Netzwerkadresse bereitstellt, und

E. ein Modul zur Übermittlung einer Netzwerkadressen-Antwortnachricht, welches veranlaßt, daß die Firewall (**30**) die Netzwerkadresse in einer Netzwerkadressen-Antwortnachricht zur Übertragung über die Verbindung an die externe Vorrichtung (**12**(m)) bereitstellt.

14. Computerprogramm-Produkt nach Anspruch 13, welches ferner ein Netzwerkadressenverwendungsmodul aufweist, welches veranlaßt, daß die externe Vorrichtung (**12**(m)) die in der Netzwerkadressen-Antwortnachricht übermittelte Netzwerkadresse beim Erzeugen von wenigstens einer Nachricht zur Übertragung an die interne Vorrichtung (**31**(s)) verwendet.

15. Computerprogramm-Produkt nach Anspruch 13 oder 14, welches ferner ein Netzwerk-Service-Provider-Steuerungsmodul aufweist, welches veranlaßt, daß die externe Vorrichtung (**12**(m)) mit dem Netzwerk (**14**) durch einen Netzwerk-Service-Provider (**11**) verbunden wird.

16. Computerprogramm-Produkt nach Anspruch 15, bei welchem das Netzwerk-Service-Provider-Steuerungsmodul ein Kommunikationssitzungsaufbaumodul umfaßt, welches veranlaßt, daß die externe Vorrichtung (**12**(m)) mit dem Netzwerk-Service-Provider (**11**) eine Kommunikationssitzung aufbaut und von diesem eine Identifizierung von einem weiteren Namen-Server empfängt.

17. Computerprogramm-Produkt nach einem der Ansprüche 13 bis 16, welches ferner ein Namen-Server-Abfragesteuerungsmodul aufweist, welches veranlaßt, daß die externe Vorrichtung (**12**(m)) eine Liste von Namen-Servern erhält, welche der externen Vorrichtung (**12**(m)) identifiziert wurden, und die Namen-Server in der Liste nacheinander in Reaktion auf eine Anfrage zum Zugriff auf eine andere Vorrichtung abfragt, wobei die Anfrage eine Sekundäradresse der anderen Vorrichtung enthält, solange bis die externe Vorrichtung (**12**(m)) eine Netzwerkadresse empfängt, und wobei die externe Vorrichtung (**12**(m)) in jedem Abfragevor-

gang eine Netzwerkadressen-Anfragesnachricht zur Übertragung über das Netzwerk (**14**) erzeugt, welche durch einen der Namen-Server in der Liste zu beantworten ist, und von diesem eine Netzwerkadressen-Antwortnachricht empfängt.

18. Computerprogramm-Produkt nach einem der Ansprüche 13 bis 17, bei welchem die Verbindung zwischen der externen Vorrichtung (**12**(m)) und der Firewall (**30**) ein Sicherheitstunnel ist, in welchem wenigstens ein Abschnitt der zwischen der externen Vorrichtung (**12**(m)) und der Firewall (**30**) übertragenen Nachrichten verschlüsselt ist.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 199 24 575 A1
Int. Cl.[6]: H 04 L 29/06
Offenlegungstag: 2. Dezember 1999

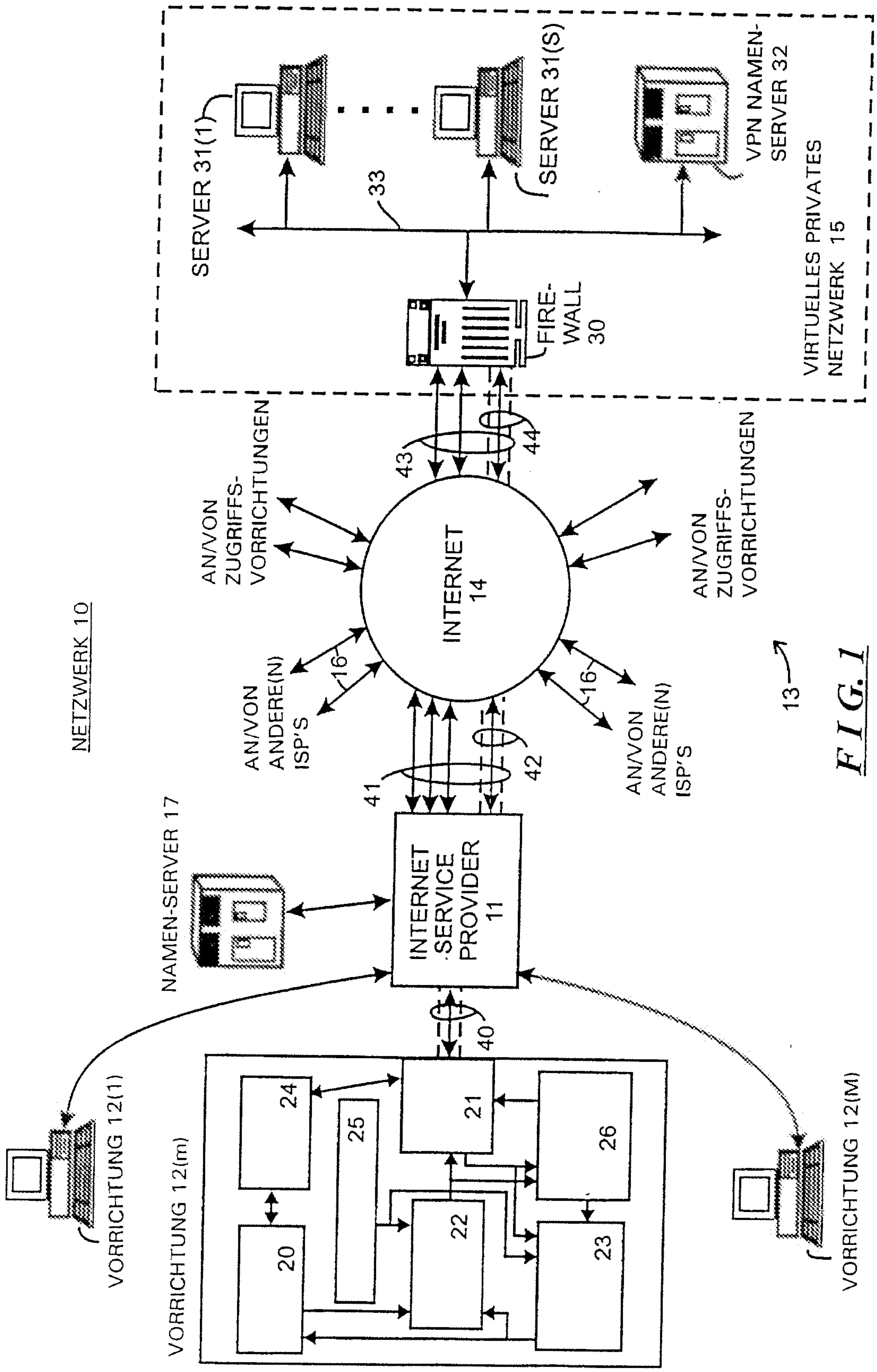


FIG. 1

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 858 189 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
22.06.2005 Bulletin 2005/25

(51) Int Cl.7: **H04L 12/46**, H04L 12/56, H04L 29/14, H04L 29/06

(43) Date of publication A2:
12.08.1998 Bulletin 1998/33

(21) Application number: **98101286.7**

(22) Date of filing: **26.01.1998**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **05.02.1997 JP 2240297**

(71) Applicant: **Hitachi, Ltd.**
Chiyoda-ku, Tokyo 101 (JP)

(72) Inventors:
- **Maciel, Frederico Buchholz**
  Kokubunji-shi, Tokyo (JP)
- **Kitai, Katsuyoshi**
  Tokyo (JP)
- **Higuchi, Tatsuo**
  Hillsboro, OR 97124 (US)
- **Yoshizawa, Satoshi**
  Musashino-shi, Tokyo (JP)
- **Murahashi, Hideki**
  Hachiouji-shi, Tokyo (JP)

(74) Representative: **Beetz & Partner Patentanwälte**
Steinsdorfstrasse 10
80538 München (DE)

(54) **Networking method**

(57) This invention provides dynamic balance of the traffic among data processing devices interconnecting networks and thereby improve the networking performance. For network traffic flowing between a first network and a second network, the traffic is distributed among the data processing devices that act as routers according to the traffic amount. An algorithm for balancing the traffic is used to select appropriate data processing devices as routers.

73 731 732 733 734 735 736

TARGET	ROUTER			NEXT HOP	PRIORITY
	ID	PHYSICAL	NETWORK		
...	...	...	...	...	...
NETWORK 1	3a	31a-P	30a-N	31a	1
	3b	31b-P	30b-N	31b	1
	3c	—	30c-N	42b	2
...	...	...	...	...	...

FIG. 6

EP 0 858 189 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 10 1286

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y	TSUCHIYA P F ED - INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: "TEAM-OF-GATEWAYS: DESIGN AND IMPLEMENTATION" CRISIS COMMUNICATIONS: THE PROMISE AND REALITY. WASHINGTON, OCT. 19 - 22, 1987, PROCEEDINGS OF THE MILITARY COMMUNICATIONS CONFERENCE. (MILCOM), NEW YORK, IEEE, US, vol. VOL. 1 CONF. 6, January 1987 (1987-01), pages 39-42, XP000619284 * paragraphs [0003] - [03.3] * -----	1-21	H04L12/46 H04L12/56 H04L29/14 H04L29/06
Y	US 5 473 599 A (LI ET AL) 5 December 1995 (1995-12-05) * abstract * -----	1-13, 19-21	
A	DEBORAH ESTRIN: "SUMMARY OF NETWORK RELATED RESEARCH ACTIVITIES" SUMMARY OF NETWORK RELATED RESEARCH ACTIVITIES, [Online] 1 March 1993 (1993-03-01), pages 1-20, XP002325498 UNIVERSITY OF SOUTHERN CALIFORNIA LOS ANGELES CA 90089-0782 USA Retrieved from the Internet: URL:http://netweb.usc.edu/papers/hpnrr.march93> [retrieved on 2005-04-20] * paragraph [01.1] * * paragraph [1.2.2.2] * * paragraph [0003] * ----- -/--	1-13, 19-21	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	27 April 2005	Dupuis, H

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

4

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 10 1286

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	ESTRIN D ET AL: "A PROTOCOL FOR ROUTE ESTABLISHMENT AND PACKET FORWARDING ACROSS MULTIDOMAIN INTERNETS" IEEE / ACM TRANSACTIONS ON NETWORKING, IEEE INC. NEW YORK, US, vol. 1, no. 1, 1 February 1993 (1993-02-01), pages 56-70, XP000362250 ISSN: 1063-6692 * pages 59-60 * * pages 62-65 * * page 68, right-hand column * -----	1-13, 19-21	
A	ESTRIN USC Y REKHTER IBM S HOTZ USC D: "A Unified Approach to Inter-Domain Routing" IETF STANDARD, INTERNET ENGINEERING TASK FORCE, IETF, CH, [Online] May 1992 (1992-05), XP015007109 IETF, INTERNET SOCIETY, 4 RUE DES FALAISES, GENEVA ISSN: 0000-0003 Retrieved from the Internet: URL:http://rfc.net/rfc2902.html> [retrieved on 2005-04-20] * paragraph [01.0] * * paragraph [2.3.2] * -----	1,19,20	TECHNICAL FIELDS SEARCHED (Int.Cl.6)
A	EP 0 324 277 A (VITALINK COMMUNICATIONS CORPORATION) 19 July 1989 (1989-07-19) * claim 1; figure all * -----	1,19,20	
A	US 5 018 137 A (BACKES ET AL) 21 May 1991 (1991-05-21) * column 2 * * columns 7-11 * -----	1	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	27 April 2005	Dupuis, H

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
& : member of the same patent family, corresponding document

4

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 10 1286

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	US 5 390 336 A (HILLIS ET AL) 14 February 1995 (1995-02-14) * column 5, line 63 - column 7, line 20 * * column 11, lines 43-57 * -----	14-18	
Y	"LOAD BALANCING FOR MULTIPLE INTERFACES FOR TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL FOR VM/MVS" IBM TECHNICAL DISCLOSURE BULLETIN, IBM CORP. NEW YORK, US, vol. 38, no. 9, 1 September 1995 (1995-09-01), pages 7-9, XP000540166 ISSN: 0018-8689 * the whole document * -----	1-18	
Y	DIAS D M ET AL: "A scalable and highly available web server" DIGEST OF PAPERS OF COMPCON (COMPUTER SOCIETY CONFERENCE) 1996 TECHNOLOGIES FOR THE INFORMATION SUPERHIGHWAY. SANTA CLARA, FEB. 25 - 28, 1996, DIGEST OF PAPERS OF THE COMPUTER SOCIETY COMPUTER CONFERENCE COMPCON, LOS ALAMITOS, IEEE COMP. SOC. PRESS,, vol. CONF. 41, 25 February 1996 (1996-02-25), pages 85-92, XP010160879 ISBN: 0-8186-7414-8 * abstract * * paragraph [0001] * * paragraph [2.1.1] * -----	1-18	TECHNICAL FIELDS SEARCHED (Int.Cl.6)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	27 April 2005	Dupuis, H

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

4

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 10 1286

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

27-04-2005

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
US 5473599	A	05-12-1995	AU	2359995	A	16-11-1995
			WO	9529544	A1	02-11-1995
EP 0324277	A	19-07-1989	US	4811337	A	07-03-1989
			AT	103745	T	15-04-1994
			AU	2830389	A	20-07-1989
			CA	1323704	C	26-10-1993
			DE	3888818	D1	05-05-1994
			DE	3888818	T2	26-01-1995
			DK	733588	A	16-07-1989
			EP	0324277	A2	19-07-1989
			IL	88799	A	21-06-1992
			JP	2005647	A	10-01-1990
			KR	9502268	B1	15-03-1995
			NO	885521	A	17-07-1989
US 5018137	A	21-05-1991	US	4972409	A	20-11-1990
			AU	600408	B2	09-08-1990
			AU	3312089	A	25-01-1990
			CA	1319185	C	15-06-1993
			DE	68921373	D1	06-04-1995
			DE	68921373	T2	19-10-1995
			EP	0349099	A2	03-01-1990
			JP	2044940	A	14-02-1990
US 5390336	A	14-02-1995	US	5129077	A	07-07-1992
			US	4814973	A	21-03-1989
			US	5978570	A	02-11-1999
			CA	1293819	C	31-12-1991
			CA	1313276	C2	26-01-1993
			CN	87106067	A ,C	09-03-1988
			DE	3751616	D1	11-01-1996
			DE	3751616	T2	09-05-1996
			EP	0262750	A2	06-04-1988
			IN	170067	A1	01-02-1992
			JP	2792649	B2	03-09-1998
			JP	63145567	A	17-06-1988
			KR	9612654	B1	23-09-1996
			WO	8801772	A1	10-03-1988
			CA	1212480	A1	07-10-1986
			DE	3486141	D1	09-06-1993
			DE	3486141	T2	19-08-1993
			EP	0132926	A2	13-02-1985
			EP	0501524	A2	02-09-1992
			EP	0495537	A2	22-07-1992
			EP	0501525	A2	02-09-1992

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 10 1286

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

27-04-2005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5390336 A		JP 2064724 C	24-06-1996
		JP 7097362 B	18-10-1995
		JP 60084661 A	14-05-1985
		JP 2538185 B2	25-09-1996
		JP 6223045 A	12-08-1994
		US 5008815 A	16-04-1991
		US 5535408 A	09-07-1996
		US 5152000 A	29-09-1992
		US 5123109 A	16-06-1992
		US 5151996 A	29-09-1992
		US 5146608 A	08-09-1992
		US 5212773 A	18-05-1993
		US 4598400 A	01-07-1986

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 836 306 A1

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
15.04.1998 Bulletin 1998/16

(51) Int. Cl.[6]: **H04L 29/06**, H04Q 11/04

(21) Application number: **96410106.7**

(22) Date of filing: **10.10.1996**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV SI

(71) Applicant:
Hewlett-Packard Company
Palo Alto, California 94304 (US)

(72) Inventors:
- **Sasyan, Serge**
  38170 Seyssinet (FR)
- **Roger, Denis**
  38760 Varces (FR)
- **Terrasse, Denis**
  38320 Eybens (FR)

(74) Representative:
Squibbs, Robert Francis
Intellectual Property Section,
Legal Department,
Hewlett-Packard France,
Etablissements de Grenoble
F-38053 Grenoble Cédex 9 (FR)

Remarks:
The application is published incomplete as filed (Article 93 (2) EPC). A claim No.7 is missing.

(54) **System providing for multiple virtual circuits between two network entities**

(57) Computers sending IP datagrams over an ATM network are generally capable of operating multiple simultaneous virtual circuits over the network. However, in doing so, they normally only set up one virtual circuit to each destination IP address so that in order to test the simultaneous operation of N virtual circuits by a computer under test, N target computers are needed. To enable a single computer (T) to provide the destination endpoints for multiple virtual circuits (SVC) from a computer (M) under test, both computers (M,T) are allocated a plurality of virtual IP addresses ($I_{M(j)}$,$I_{T(i)}$) and the target computer (T) is additionally provided with a module running address-changing processes (70,71) that avoids the IP layers (20) of both computers from rejecting IP datagrams (25A,25B) addressed with the virtual IP addresses. As a result, each computer (M,T) can be addressed with any of a plurality of IP addresses and each will result in the creation of a respective virtual circuit (SVC) between the computers (M,T).

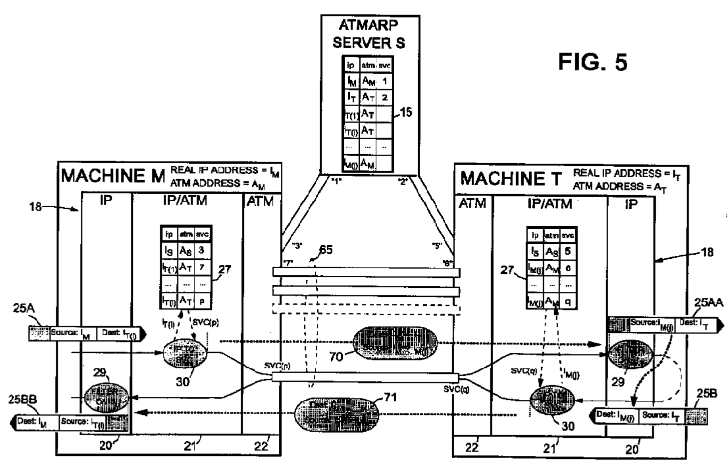


FIG. 5

EP 0 836 306 A1

Printed by Xerox (UK) Business Services
2.15.12/3.4

Description

Field of the Invention

The present invention relates to a system providing for multiple virtual circuits between two network entities for use in particular, but not exclusively, in the testing of network node apparatus providing IP messaging over an ATM network.

Background of the Invention

As is well-known, the Internet Protocol (IP) uses a scheme of IP addresses by which every connection of a node to the Internet has a unique IP address. IP addresses are high-level addresses in the sense that they are independent of the technology used for the underlying network to which a node is connected. Each node will also have a low-level, network-dependent address (often callled the MAC address) that is actually used for addressing at the network level and the IP protocol suite includes a address reolution protocol (ARP), logically positioned below the IP layer itself, that is responsible for translating between IP addresses contained in a message and the local MAC addresses.

An increasingly important technology for local area networks is ATM. ATM (Asynchronous Transfer Mode) is a multiplexing and switching technique for transferring data across a network using fixed sized cells that are synchronous in the sense that they appear strictly periodically on the physical medium. Each cell comprises a payload portion and a header, the latter including a label that associates the cell with an instance of communication between sending and receiving network end systems; this instance of communication may involve the transfer of many cells from the sending end system, possibly to multiple receiving end systems. ATM is asynchronous in the sense that cells belonging to the same instance of communication will not necessarily appear at periodic intervals.

In ATM, the labels appended to the cells are fixed-size context dependent labels, that is, they are only understandable in the light of context information already established at the interpreting network node, the label generally being replaced at one node by the label required for the next node. In other words, ATM is a virtual circuit technology requiring a set up phase for each instance of communication to establish the appropriate label knowledge at each node. Of course, to set up a desired communication, it is still necessary to identify uniquely the nodes forming the communication end points and this is achieved by using ATM addresses, generally of a significance limited to the particular ATM network concerned.

The process of sending IP messages (datagrams) over a ATM network, including the operation of the required ATM ARP system, is set out in RFC 1577 of the IETF Internet Engineering Task Force) dated January 1993. This RFC assumes an arrangement in which a sending node will only establish a single vircuit circuit to a given destination IP address (of course, this one vircuit circuit may carry multiple connections between respective pairings of high-level end points in the nodes).

Figure 1 of the accompanying drawings is a diagram illustrating the basic mechanism by which two machines M and T exchange IP datagrams over a switched virtual circuit (SVC) established across an ATM network. The machines M and T have respective IP addresses I_M and I_T and respective ATM addresses A_M and A_T; each machine knows its own addresses. An ATMARP server S knows the IP and ATM addresses of all active nodes on the network, including machines M and T; more particularly, server S maintains an ARP table 15 associating the IP address of each node with its ATM address. The server S maintains open a respective SVC (switched virtual circuit) to each active node and the identity of this SVC is held in the ARP table 15; thus, in the Figure 1 example, the server S is in communication with machine M over an SVC identified as SVC "1" at the server, and the server S is in communication with machine T over an SVC identified as SVC "2" at the server S. At machines M and T these virtual circuits are independently identified - thus at machine M its SVC to the server S is identified as SVC "3" whilst at machine T its SVC to the server S is identified as SVC "5".

The communications interface 18 in each of the machines M and T comprises three main layers, namely: an IP layer 20 responsible for forming IP datagrams (including source and destination IP addresses) for transmission ad for filtering incoming datagrams; an intermediate IP/ATM layer 21 for determining the SVC corresponding to the destination IP address of an outgoing datagram; and an ATM layer 22, including the low-level network interface hardware, for sending and receiving datagrams packaged in ATM cells over SVCs.

The IP/ATMlayer 21 maintains an ARP cache table 27 which like the table 15 of the server S contains associations between IP address, ATM address and SVC. Thus, table 27 of machine M contains an entry of the IP address I_S, ATM address A_S, and SVC identity "3" for the server S, and similarly, table 27 of machine T contains an entry of the IP address I_S, ATM address A_S, and SVC identity "5" for the server S. The cache table 27 only holds information relevant to current SVCs of the machine concerned so that during the initial establishment of a SVC to a new destination, the cache table must be updated with relevant information from the ATMARP server S; this general process will be described in more detail hereinafter with reference to Figure 2. For the present, it will be assumed that an SVC has already been established between machines M and T and that the cache tables contain the relevant information (in particular, cache table 27 of machine M contains an entry with the IP address I_T, ATM address A_T, and SVC identity "4" for machine T, and cache table

27 of machine T contains an entry with the IP address I_M, ATM address A_M, and SVC identity "9" for machine M).

Considering now the case of a high-level application in machine M wanting to send a message to machine T, this application passes the message to the IP layer 20 together with the destination IP address I_T. IP layer 20 packages the message in one (or more) datagrams 25A with a destination IP address of I_T and source I_P address of I_M. Datagram 25A is then passed to the IP/ATM layer 21 which executes an IP-to-SVC lookup task 30 to determine from table 27 the SVC to be used for sending the datagram to its destination address I_T; in the present case, table 27 returns the SVC identity "4" and the layer 21 passes this identity together with the datagram 25A to the ATM layer 22 which then sends the datagram in ATM cells on SVC "4". The datagram is in due course received by machine T and passed up by layers 22 and 21 to the IP layer 20 where a filtering task 29 determines from the datagram destination address that the datagram is indeed intended for machine T; the contents of the datagram are then passed to the relevant high-level application. In the present example, this high-level application produces a reply message which it passes to the IP layer 20 together with the required return address, namely the source IP address in the received datagram 25A. IP layer 20 generates datagram 25B with the received return address as the destination address, the IP address I_T of machine T being included as the source address. The datagram 25B is passed to IP/ATM layer 21 where IP-to-SVC lookup task 30 determines from cache table 27 that the required destination can be reached over SVC "9". This information together with datagram 25B is then passed to ATM layer 22 which transmits the datagram in ATM cells over SVC "9" to machine M. When the datagram is received at machine M it is passed up to the IP layer 20 where it is filtered by task 29 and its contents then passed on to the relevant high-level application.

Figure 2 of the accompanying drawings illustrates in more detail the functioning of the IP/ATM layers 21 of machines M and T in respect of datagram transmission from machine M to machine T, it being appreciated that the roles of the two layers 21 are reversed for transmission in the opposite direction. More particularly, upon the IP-to-SVC lookup task 30 being requested to send a datagram to IP address I_T, it first carries out a check of the cache table 27 (step 31) to determine if there is an existing entry for I_T (and thus an SVC, assuming that entries are only maintained whilst an SVC exists). Step 32 checks the result of this lookup - if an SVC already exists (in this case, SVC "4"), then step 39 is executed in which the datagram is passed together with the identity of the relevant SVC to the ATM layer 22; however, if the lookup was unsuccessful, task 30 executes steps 33 to 38 to set up an SVC to destination I_T before executing step 39.

The first step 33 of the setup process involves the sending of an ARP request to the ATMARP server S over the relevant SVC requesting the ATM address corresponding to I_T. Server responds with ATM address A_T which is received by task 30 at step 34.

Task 30 now updates the cache table 27 with the IP address I_T and ATM address A_T (step 35). Next, task 30 requests (step 36) the ATM layer 22 to establish a new SVC to ATM address A_T and this initiates an SVC setup process 28 which may be executed in any appropriate manner and will not be described in detail herein. In due course, process 28 returns the identity of the SVC that has been set up to A_T (in this case, SVC "4"), this identity being received at step 37 of task 30. Finally, cache table 30 is updated at step 38 by adding the SVC identity ("4") to the entry already containing I_T and A_T.

In machine T, the setup of the new SVC to the machine from machine M is handled by the setup process 28 of machine T. The process 28 informs the IP/ATM layer that a new SVC has been setup and this triggers execution of an update task 40 to update the cache table 27 of machine T. More particularly, on the new SVC indication being received (step 41), a first update step 42 is carried out to add an entry to the table confining the identity of the new SVC (in the present example "9"), and the ATM address A_M of the node at the other end of the SVC; at this stage, the corresponding IP address is not known to machine T. In order to obtain this IP address, an inverse ARP request is now made to machine M (step 43). In due course a response is received (step 44) containing the IP address of machine M. The cache table 27 is then updated at step 45 with the IP address I_M of machine M and the IP/ATM layer is now ready to effect IP-to-SVC translations for datagrams intended for machine M.

The inverse ARP request sent by machine T to machine M is handled by an inverse ARP task 50 that examines the request (step 51) and on finding that it contains the ATM address A_M, responds with the IP address I_M of machine M (step 52).

To facilitate explanation of the preferred embodiment of the invention hereinafter, the messages across the boundary between the IP/ATM layer 21 and the ATM layer 22 have been labelled in Figure 2 as follows where superscript "T" indicates an outgoing message (that is, from the IP/ATM layer to the ATM layer) and the superscript "R" indicates incoming messages (that is, from the ATM layer to the IP/ATM layer):

- $X1^T$ - outgoing ARP request;
- $X2^R$ - incoming ARP response;
- $X3^T$ - outgoing SVC setup request;
- $X4^R$ - incoming SVC setup done indication;
- $X5^R$ - incoming new SVC indication;
- $X6^T$ - outgoing INARP request;
- $X6^R$ - incoming INARP request;
- $X7^T$ - outgoing INARP response;
- $X8^T$ - outgoing datagram;
- $X8^R$ - incoming datagram.

It will be appreciated that machines connecting to an ATM network, such as machines M and T as well as the server S, are designed to handle a large number of virtual circuits simultanteously. If in testing such a machine (machine M in the following discussion) it is desired to fully stress the machine under test, then the design limit of concurrently operating virtual circuits must be simultaneously used. However, as already indicated, current practice is that only one virtual circuit is established to each distinct IP address. As a result, since generally each machine that might be used to test machine M has only one network connection and therefore only one IP address, if machine M is designed to operate up to N virtual circuits simultaneously, then it requires N machines to test machine M. Such an arrangement is illustrated in Figure 3 where the N machines are constituted by the server S and (N-1) other machines here represented as machines T1 to T(N-1). Such an arrangement is generally impractical as N may be as high as 1024 or more.

It is an object of the present invention to provide a mechanism that enables, inter alia, the foregoing test problem to be overcome.

Summary of the Invention

According to the present invention, there is provided a system in which a plurality of entities are connected to a network ad can exchange messages across virtual circuits set up over the network between said entities, each entity having a operative high-level address on the network, and each entity comprising:

-- high-level messaging means for handling message transmission and receipt on the basis of the aforesaid high-level addresses, the high-level messaging means comprising means for including in outgoing messages the operative high-level address of the entity as a source identifier and the operative high level address of the intended recipient entity as a destination identifier, and means for filtering incoming messages according to the destination identifier contained in the message:

-- virtual-circuit means for providing virtual circuits between the entity and other entities, there being a respective virtual circuit for each different destination identifier in use, and

-- intermediate means for passing an outgoing message from the high-level messaging means to that one of the virtual circuits provided by the virtual-circuit means which corresponds to the destination identifier of the message;

characterised in that each of a first and a second one of the entities has a plurality of virtual high-level addresses associated with it that are different from the operative high-level address of the entity, the virtual high-level addresses being usable by the messaging means of the first and second entities as destination identifiers in outgoing messages; **and in that** between the intermediate means of the first and second entities, there are provided address-changing means responsive to each of at least some of the messages sent between these entities with a said virtual high-level address as its destination identifier, to change that address to the operative high-level address of the corresponding entity and to change the operative high-level address provided as the source identifier of the message into one of the said virtual high-level addresses associated with the sending entity in dependence on the virtual high-level address initially provided as the destination identifier of the same message.

By virtue of this arrangement, it is possible to establish a plurality of virtual circuits between the first and second entities by using the different virtual high-level addresses of the entities as the destination identifiers in messages exchanged between the entities, the receiving high-level adressing means accepting such messages due to the address-changing means having changed the destination identifier to the operative high-level address of the receiving entity. By also changing the source identifier, it is possible to retain in the message information sufficient to associate any reply message with a particular one of the virtual circuits established with the sending entity (in particular, the reply message can be sent back over the same virtual circuit as the message to which it is a reply - however, if desired, it is also possible to use a separate virtual circuit for the reply messages).

Preferably, the address-changing means comprises first address-changing functionality for effecting the aforesaid changes for messages sent from the first entity to the second entity, and second address-changing functionality for effecting these changes for messages sent from the second entity to the first entity, both the first and second address-changing functionalities being provided in the second entity. This configuration is well suited for testing the ability of network node apparatus to concurrently operate a plurality of virtual circuits where the network node apparatus is operative to establish a virtual circuit for each different high-level destination address being handled; more particularly, the network node apparatus serves as the aforesaid first entity, and is caused to send messages to at least some of the vial high-level addresses associated with the second entity. By placing the address-changing means in the second entity, no modifications are needed to the network node apparatus in order for it to be able to establish a plularity of virtual circuits with the second entity.

Advantageously, the address-changing means effects a predetermined transformation on the virtual high-level address forming the initial destination identifier of a said message in order to form the virtual high-level address to be used for the source identifier of that message. For example, this transformation may simply involved changing the address by one (where the address is numeric in form).

The present invention is particularly applicable to systems in which the high-level addresses are IP addresses and the network is an ATM network.

Brief Description of the Drawings

A system embodying the invention will now be described, by way of non-limiting example, with reference to the accompanying diagrammatic drawings, in which:

- **Figure 1** is a diagram of a known system for sending IP datagrams over a ATM network between two machines M and T;
- **Figure 2** is a diagram illustrating the steps carried out by the Figure 1 system in establishing a virtual circuit between machines M and T;
- **Figure 3** is a diagram of a known test arrangement for testing the ability of a machine M to concurrently operate multiple virtual circuits;
- **Figure 4** is a diagram showing a test arrangement embodying the invention for testing the ability of a machine M to concurrently operate multiple virtual circuits;
- **Figure 5** is a diagram similar to Figure 1 but showing a system embodying the invention in which multiple virtual circuits are established between machines M and T;
- **Figure 6** is a diagram illustrating the processing effected by a module VNS disposed in machine T of the Figure 5 system when machine M initiates the opening of a new virtual circuit between machines M and T; and
- **Figure 7** is a diagram illustrating the processing effected by a module VNS disposed in machine T of the Figure 5 system when machine T initiates the opening of a new virtual circuit between machines M and T.

Best Mode of Carrying Out the Invention

The embodiment of the invention now to be described provides a system in which it is possible to establish a plurality of SVCs (switched virtual circuits) across an ATM network for the exchange of IP datagrams between two machines M and T whereby it is possible to test the ability of machine M to concurrently operate a plurality of virtual circuits without needing to provide a respective destination machine for each SVC operated by machine M. The overall test arrangement is illustrated in Figure 4 where machine M operates N SVCs over ATM network 10, one SVC being with ATMARP server S and (N-1) SVCs being with machine T. According to the preferred embodiment, the establishment of multiple concurrent SVCs between machine M and T is effected without modification to machine M.

Figure 5 shows a system embodying the present invention, this system being similar to that of Figure 1 but being operative to provide a plurality of concurrent SVCs 65 between machines M and T. In the Figure 5 system, the machines M and T and the server S are assumed to operate in the same way and have the same IP and ATM addresses as in Figure 1; in addition, in Figure 5 the same SVCs are established between the server S and the machines M and T as in Figure 1. The Figure 5 system includes, however, added functionality provided by processes 70 and 71 which in Figure 5 are shown independent of machines M and T but in practice would be provided either distributed between machines M and T or wholly in one of these machines; in a preferred embodiment, the processes 70 and 71 are provided in machine T.

In accordance with the present invention, each machine M and T is allocated a number of virtual IP addresses different from its operative (or "real") IP address (this latter address being the one which the IP layer knows about for inclusion as the source address in outgoing datagrams and upon which filtering is carried out by task 29). Thus, machine M is allocated virtual IP addresses $I_{M(1)}$, $I_{M(2)}$,......$I_{M(j)}$...; similarly, machine T is allocated virtual IP addresses $I_{T(1)}$, $I_{T(2)}$,......$I_{T(i)}$....

Each of these virtual IP addresses is entered into table 15 of ATMARP server S together with the ATM address of the corresponding one of the machines M,T; thus virtual IP address $I_{M(j)}$ is associated with ATM address A_M and virtual IP address $I_{T(i)}$ is associated with ATM address A_T.

Now, if the communications interface 18 of machine M is asked to send a message to IP address $I_{T(i)}$, IP layer 20 will construct a datagram 25A having a destination address of $I_{T(i)}$ and a source address of I_M. The IP-to-SVC task 30 of IP/ATM layer 21 then acts in the manner already described to fetch the ATM address corresponding to $I_{T(i)}$ from server S and set up an SVC (here identified by "p") towards machine T; the cache table 27 is updated appropriately. The datagram 25A is now sent by ATM layer over SVC(p) to machine T.

If no further action is taken, the datagram 25A, after receipt at machine T, will be rejected by the filter task 29 as the destination address $I_{T(i)}$ of the datagram differs from the operative IP address I_T known to task 29 of machine T. Accordingly, a process 70 is provided that recognises the destination address of datagram 25A as being a virtual IP address of machine T and substitutes the real IP address of machine T for the virtual address in the destination field of the datagram 25A. The datagram will now be allowed through by filter task 29 of machine T.

However, a further difficultly remains. If only the destination address is changed, the resultant datagram contains no indication that the datagram was not ordinarily sent with the real IP address of machine T; any reply will therefore be sent on an SVC set up to take datagrams from machine M to the real IP address of machine M. This SVC would end up taking all the reply messages for messages sent from machine M to machine T over all the SVCs set up in respect of the virtual IP addresses allocated to machine T. This is clearly undesirable. To avoid this, the source address of datagram 25A is also changed by process 70. More particularly, the source address is changed from the real IP address of machine M to one of the virtual IP addresses $I_{M(j)}$ of this machine, the virtual address chosen being dependent on the original virtual IP address forming the destination address of the datagram. As a result, all datagrams 25A having the same virtual destination address end up after operation of process 70 as datagrams 25AA with the same virtual source address, whereas datagrams 25A having different initial virtual destination addresses end up as datagrams 25AA with different source addresses. The process of changing the source address preferably involves a predetermined transformation of the virtual destination address - for example, to obtain the required virtual source address, the virtual destination address can simply be incremented by one (there would thus exist, for example, a set of even virtual IP addresses for machine M and a corresponding set of odd virtual IP addresses for machine T, each even virtual IP address of machine M being associated with the immediately adjacent, lower-valued, odd virtual IP address of machine T).

The address-changing process 70 must be carried out on datagram 25A after operation of the IP-to-SVC task 30 in machine M and prior to the filter task 29 in machine T. In addition, whilst the two address-hanging operations of process 70 need not be carried out at the same time or at the same location (though it is, of course, convenient to do so), the changing of the source address must be done whilst the initial virtual destination address is still available.

The contents of datagram 25AA are passed by IP layer 20 of machine T to a high-level application which, in the present example, produces a reply that it passes to layer 20 for sending back to IP address $I_{M(j)}$, that is, to the source address contained in datagram 25AA. Layer 20 produces a datagram 25B with source address I_T and destination address $I_{M(j)}$. Next, IP-to-SVC task 30 of layer 21 looks up the destination address in the cache table 27 to find out the SVC to be used for the reply. If, as will normally be the case, the same SVC is to be used for the reply as carried the original datagram 25A with destination address $I_{T(i)}$, then the SVC setup process will have been arranged to enter the address $I_{M(j)}$ in cache table 27 against that SVC (in present case, identified to machine T by "q"); a lookup on $I_{M(j)}$ will thus return "q" as the required SVC. However, if it is desired to use a different SVC for datagrams 25B passing from T to M as used for datagrams 25A passing from M to T, then the first lookup on $I_{M(j)}$ by task 30 will not identify an SVC and task 30 must then initiate set up of a new SVC.

Assuming that the same SVC is to be used for the datagrams 25B with destination address $I_{M(j)}$ as for the datagrams 25A with destination address $I_{T(i)}$, then alter task 30 has identified SVC(q) as the appropriate SVC, the datagram 25B is passed to the ATM layer 22 for sending out over SVC(q). In due course, machine M receives this datagram and passes it up to IP layer 20; however, before the datagram reaches this layer, it must undergo address-change processing similar to that carried out on datagram 25A. More particularly, the virtual destination address $I_{M(j)}$ must be changed to the real IP address I_M of machine M, and the real source address I_T of machine T must be changed to the virtual IP address $I_{T(i)}$ of machine T associated with the virtual destination address $I_{M(j)}$. This address-change processing is carried out by process 71.

With regard to the source address change, where the corresponding change was effected for datagram 25A by incrementing by one the virtual destination address $I_{T(i)}$ of that datagram, then for datagram 25B, the source address is changed to the destination address $I_{M(j)}$ decremented by one.

In a similar manner to process 70, process 71 must be carried out on datagram 25B after operation of the IP-to-SVC task 30 in machine T and prior to the filter task 29 in machine M. In addition, whilst the two address-changing operations of process 71 need not be carried out at the same time or at the same location, the changing of the source address must be done whilst the initial virtual destination address is still available.

Following operation of process 71, datagram 25BB with source address $I_{T(i)}$ and destination address I_M is allowed through by filter task 29 and the contents of the datagram are passed to the relevant high-level application.

Having described the general mechanism by which virtual IP addresses can be used for exchanging datagrams 25A and 25B across a SVC between machines M and T, the issue will now be addressed as to how the cache table 27 in machine T is updated on SVC setup to associate the new SVC (that is, SVC(q) at machine T) with the virtual IP address $I_{M(j)}$ of machine M (this is required where the same SVC is to be used for the reply datagram 25B as for the original datagram 25A). It will be appreciated that when the task 40 (see Figure 2) is executed, the INARP request sent to machine M will only return the real IP address I_M of machine M, there being no other information available to the update task 40 by which any other result could be obtained from the INARP task 50; clearly, something additonal needs to be done for update task 40 to be able to associate the virtual IP address $I_{M(j)}$ with the newly created SVC(q) in table 27. In fact, there are a number of ways in which the update task could be informed that the IP address to be associated with SVC(q) is $I_{M(j)}$. For example, the update task 40 could be arranged to send a request back over the newly-created SVC(q) asking machine M to identify the destination IP address $I_{T(i)}$ it associates with that SVC; from this information, the update task could determine the associated virtual IP address $I_{M(j)}$ of machine M (assuming there is a predetermined relation between the two as is the case in the described embodiment) and then update table 27 accordingly. An alternative approach that avoids sending a special request to machine M is to wait for machine M to supply the destination IP address $I_{T(i)}$ in the first IP datagram 25A sent over the new SVC(q), the update task then deriving the required address $I_{M(j)}$ as described above.

A variant of this latter approach is to leave the update task 40 unchanged but provide an additional process that:

(a) delays the INARP request until the destination address $I_{T(i)}$ of the first datagram from machine M to machine T can be captured;
(b) uses the captured address $I_{T(i)}$ as the source address of the INARP request that is now sent on to machine M.

The INARP response from machine M will therefore have a destination address $I_{T(i)}$ and a source address (that forms the substance of the INARP response) of I_M. By ensuring that this response datagram is subject to the processing effected by process 70, the source data in the INARP response will be changed to $I_{M(j)}$ by the time the response reaches the update task 40. Thus, the required updating of the table 27 of machine T can be achieved without modification to the existing tasks of machines M and T but simply by the addition of a further process for effecting steps (a) and (b) described above. This approach is the preferred one for updating table 27 and is the one used in the module described below with reference to Figures 6 and 7.

The above-described system involving the allocation of multiple virtual IP addresses to machines M and T and the provision of the address-changing processes 70 and 71, permits multiple SVCs to be concurrently operated between the machines M and T thereby enabling implementation of the test arrangement depicted in Figure 4. Of course, when testing the machine M, it is desirable that no changes are made to this machine; accordingly, it is preferred for such a test arrangement to implement the address-changing processes 70 and 71 in machine T.

The implementation of the address-changing processes 70 and 71, and of the INARP request modification process, can conveniently by done by inserting a module (hereinafter called the VNS module) between the IP/ATM layer 21 and the ATM layer 22 of machine T; in fact, an instance of this module is created for each SVC, this being relatively easy to implement when using a STREAMS type I/O implementation as provided in most UNIX systems (conveniently one stream is provided for each SVC and the VNS module is pushed onto each stream when the stream is created).

The messages passing across the boundary between layers 21 and 22 have already been described above with reference to Figure 2 and the processing effected by the VNS module on each of these messages will next be described. First, the situation of Figure 5 will be considered where it is machine M that initiates the setting up of a new SVC to machine T. The first message received by the VNS module will be the SVC setup indication message $X5^R$ and this is passed through the VNS module without modification (see Figure 6). Next, the INARP request $X6^T$ is received and is subject to the modification process 82 described above, namely it is delayed until the first IP datagram 25A is received and the address $I_{T(i)}$ extracted and used for the source address of the INARP request. The INARP response $X7^R$ is then received and subject to the address-changing process 70.IP datagrams $X8^R$ from machine M to machine T are also subject to the address-changing process 70. IP datagrams $X8^T$ from machine T to machine M are subject to address-changing process 71.

Figure 7 depicts the processing effected by the VNS module in the situation where it is the machine T rather than the machine M that initiates SVC setup. The messages passing through the VNS module in this case are those shown crossing the boundary between layers 21 and 22 in Figure 2 for machine M. The first four messages $X1^T$, $X3^T$, $X2^R$, and $X4^R$ are passed through without modification. The INARP request received from machine M is subject to the modification process 82, being delayed until the destination address of the first IP datagram from machine T to machine M can be captured and used as the source address of the INARP request. The INARP response $X7^T$ is subjected to process 71 as are IP datagrams $X8^T$ from machine T to machine M. IP datagrams $X8^R$ from machine M to machine T are subjected to process 70.

It will be appreciated that many variants are possible to the above-described embodiment of the invention. It will also be appreciated that the invention is not limited to switched virtual circuits but can equally be applied to permanent virtual circuits. Furthermore, the setting up of multiple virtual circuits between two machines can be used not only for implementing the test arrangement described above with reference to Figure 4 but also for other purposes.

Although the present invention has been described in the context of high-level addresses constituted by IP addresses and virtual circuits set up across an ATM network, the invention can be applied to other types high-level addresses and other types of virtual-circuit network. For example, the high-level addresses could be MAC addresses in the case of a network in the form of a emulated LAN (ELAN) over an ATM network.

Claims

1. A system in which a plurality of entities are con-

nected to a network and can exchange messages across virtual circuits set up over the network between said entities, each entity having an operative high-level address on the network, and each said entity comprising:

-- high-level messaging means for handling message transmission and receipt on the basis of said high-level addresses, said high-level messaging means comprising means for including in outgoing ones of said messages the operative high-level address of the entity as a source identifier and the operative high level address of the intended recipient entity as a destination identifier, and means for filtering incoming ones of said messages according to the destination identifier contained in the message:
-- virtual-circuit means for providing virtual circuits between the entity and other said entities, there being a respective virtual circuit for each different destination identifier in use, and
-- intermediate means for passing an outgoing message from said high-level messaging means to that one of the virtual circuits provided by the virtual-circuit means which corresponds to the destination identifier of the message;

characterised in that each of a first and a second said entity has a plurality of virtual high-level addresses associated with it that are different from said operative high-level address of the entity, said virtual high-level addresses being usable by the messaging means of said first and second entities as destination identifiers in outgoing messages; **and in that** between said intermediate means of said first and second entities, there are provided address-changing means responsive to each of at least some of said messages sent between these entities with a said virtual high-level address as its destination identifier to change that address to the said operative high-level address of the corresponding entity, and to change the operative high-level address provided as the source identifier of the message into one of the said virtual high-level addresses associated with the sending entity in dependence on the virtual high-level address initially provided as the destination identifier of the same message.

2. A system according to claim 1, wherein said address-changing means effects a predetermined transformation on the virtual high-level address forming the initial destination identifier of a said message to which the address-hanging means is responsive in order to form the virtual high-level address to be used for the source identifier of that message.

3. A system according to claim 2, wherein said address-changing means is responsive to messages sent in both directions between said first and second entities with virtual high-level addresses as destination identifiers, the said transformation effected in respect of such messages sent in one said direction being the reverse of the transformation effected in respect of other such messages sent in the opposite said direction.

4. A system according to claim 1, wherein said address-changing means comprises first address-changing functionality for effecting said changes for messages sent from said first entity to said second entity, and second address-changing functionality for effecting said changes for messages sent from said second entity to said first entity, both said first and second address-changing functionalities being provided in said second entity.

5. A system according to claim 1, wherein said address-changing means comprises first address-changing functionality for effecting said changes for messages sent from said first entity to said second entity, and second address-changing functionality for effecting said changes for messages sent from said second entity to said first entity, the two said address-changing functionalities being provided in respective ones of said first and second entities.

6. A system according to claim 1, wherein:

-- each said entity has a low-level address on the network;
-- said intermediate means of each entity further comprises:

-- first association means for providing an association between the destination identifier of a outgoing message and the low-level address of the corresponding said entity,
-- second association means for providing an association between the destination identifier of an outgoing message and a said virtual circuit,

said intermediate means using its second association means to identify from the destination identifier of a said outgoing message which virtual circuit is to be passed the message where such virtual circuit exists, and otherwise first passing a request to the said virtual circuit means of the same entity to establish a virtual circuit to the entity having the low-level address identified by said first association means as associated with the destination identifier of the outgoing message; and

-- the said virtual-circuit means of each entity includes setup means responsive to a said request from the intermediate means of the same entity to establish a virtual circuit to the said entity having the low-level address provided in said request, said setup means causing the intermediate means to update its second association means to associate the newly-established virtual circuit with the said destination identifier relevant to said request;

the first association means of each of said first and second entities serving to provide an association between the virtual high-level addresses of the other of said first and second entities and the low-level address of that other entity.

8. A system according to claim 7, further comprising a network server containing associations between high-level addresses and low-level addresses, said first association means of each said entity comprising means for interrogating said network server for a required association.

9. A system according to claim 7, wherein said second association means comprises cache means for temporarily holding said associations between said destination identifiers and currently corresponding virtual circuits.

10. A system according to any one of claims 1 to 9, wherein said high-level addresses are IP addresses and said network is a ATM network.

11. A system according to any one of claims 1 to 9, wherein said high-level addresses are MAC addresses and said network is a emulated LAN over an ATM network.

12. A method of testing the ability of network node apparatus to operate a plurality of virtual circuits at the same time, said network node apparatus being arranged to establish a virtual circuit for each different high-level destination address being handled, said method involving setting up a system according to claim 4 with said network node apparatus as said first entity, and causing the network node apparatus to send messages to at least some of said virtual high-level addresses associated with said second entity.

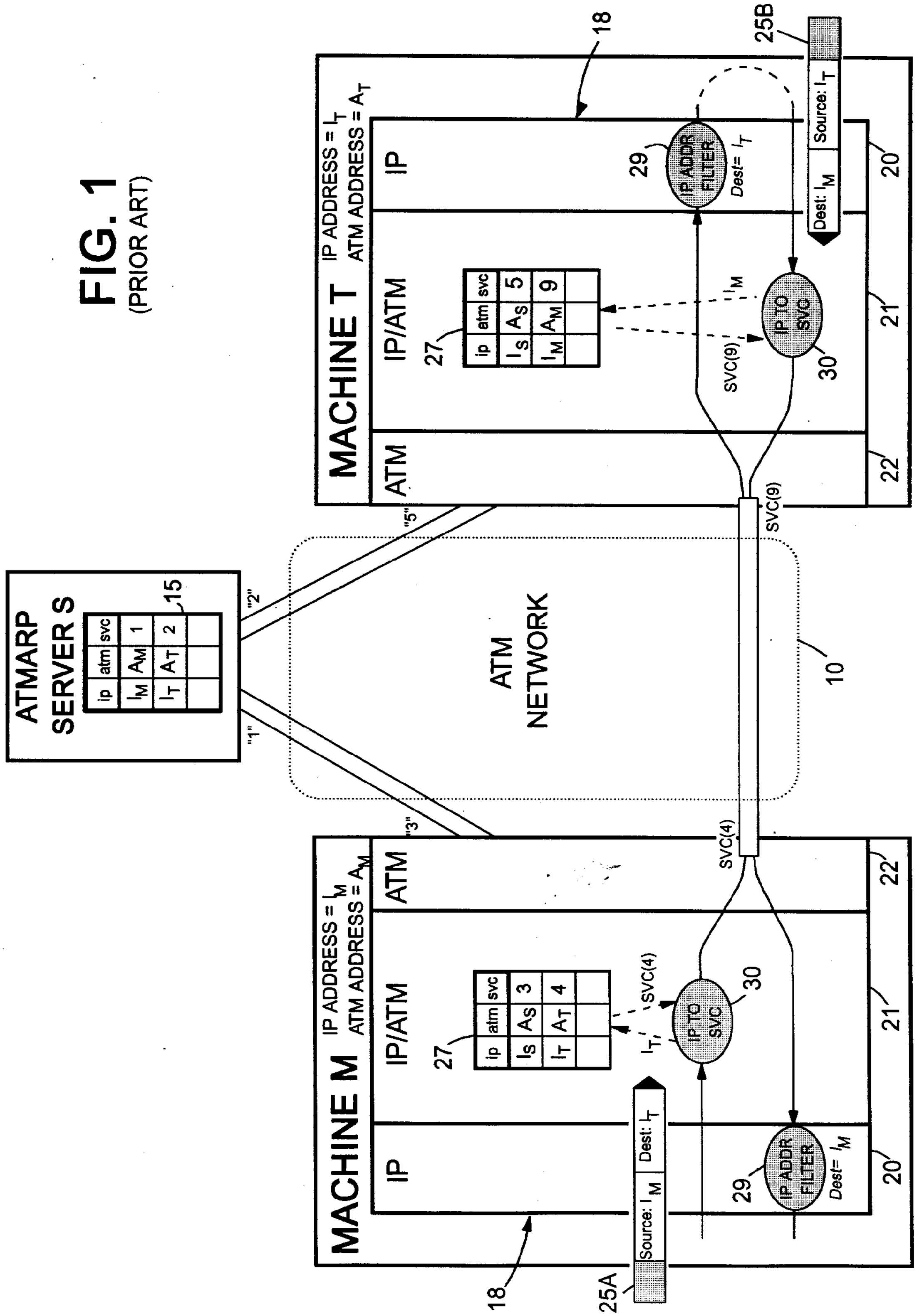


FIG. 1
(PRIOR ART)

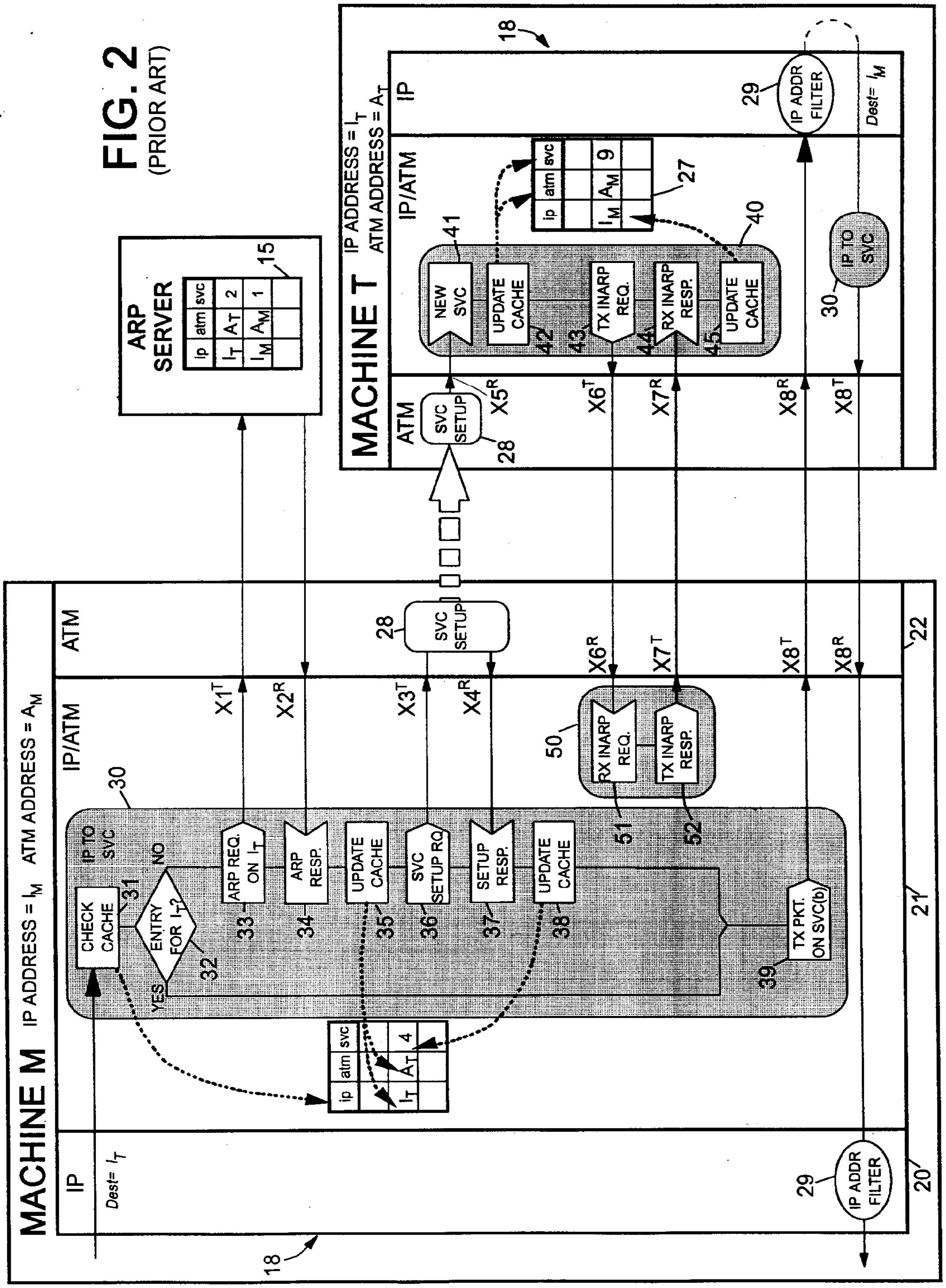


FIG. 2
(PRIOR ART)

FIG. 3
(PRIOR ART)

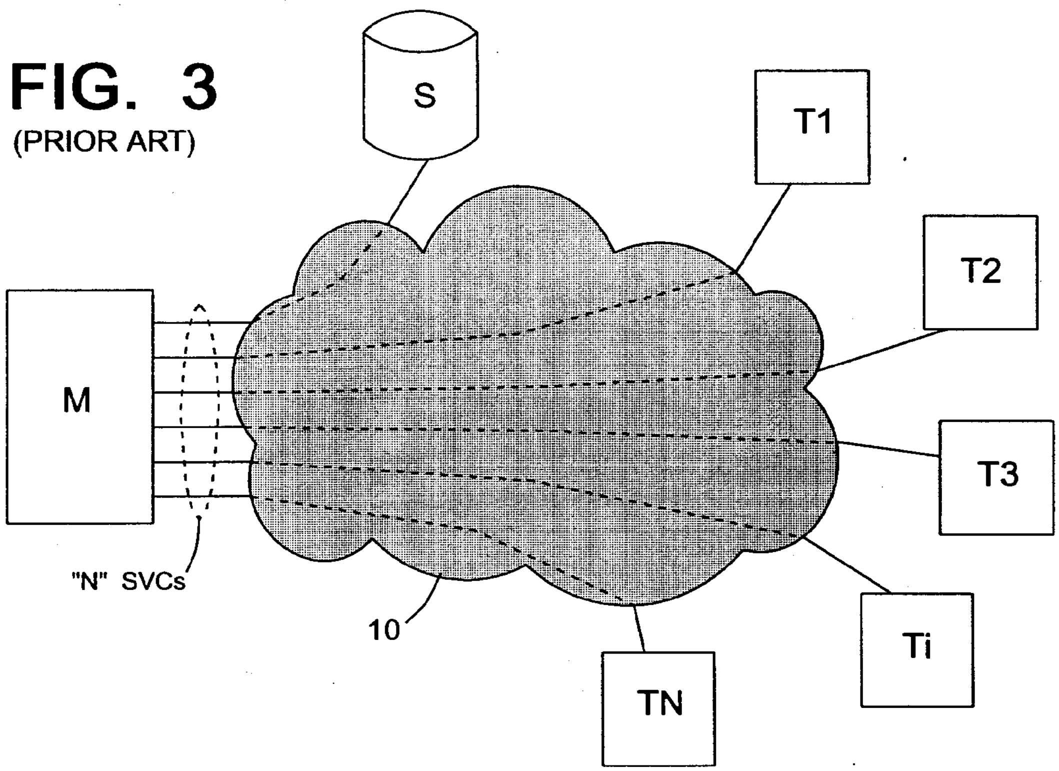


FIG. 4

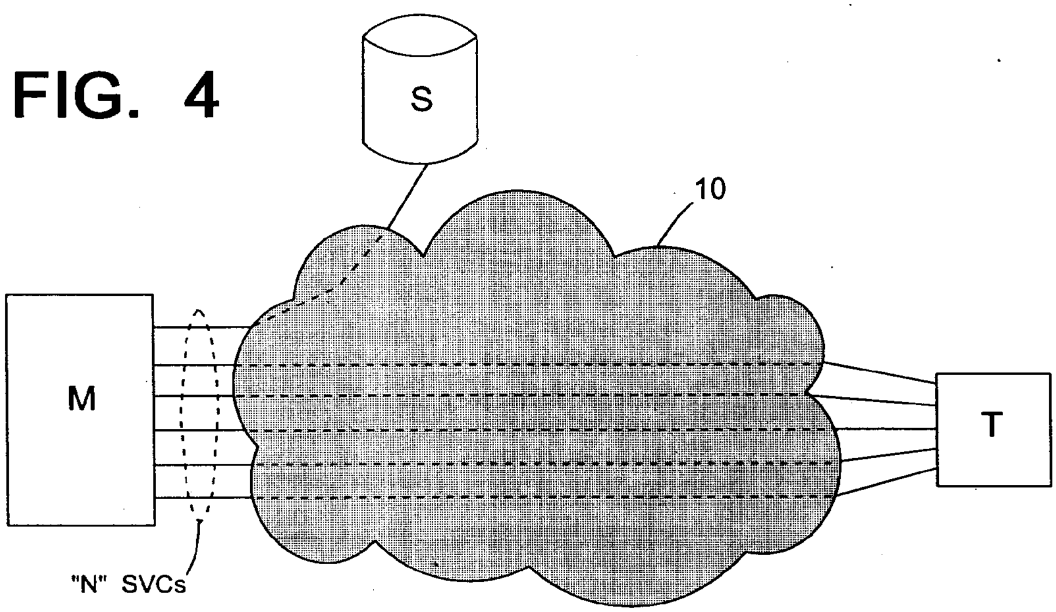
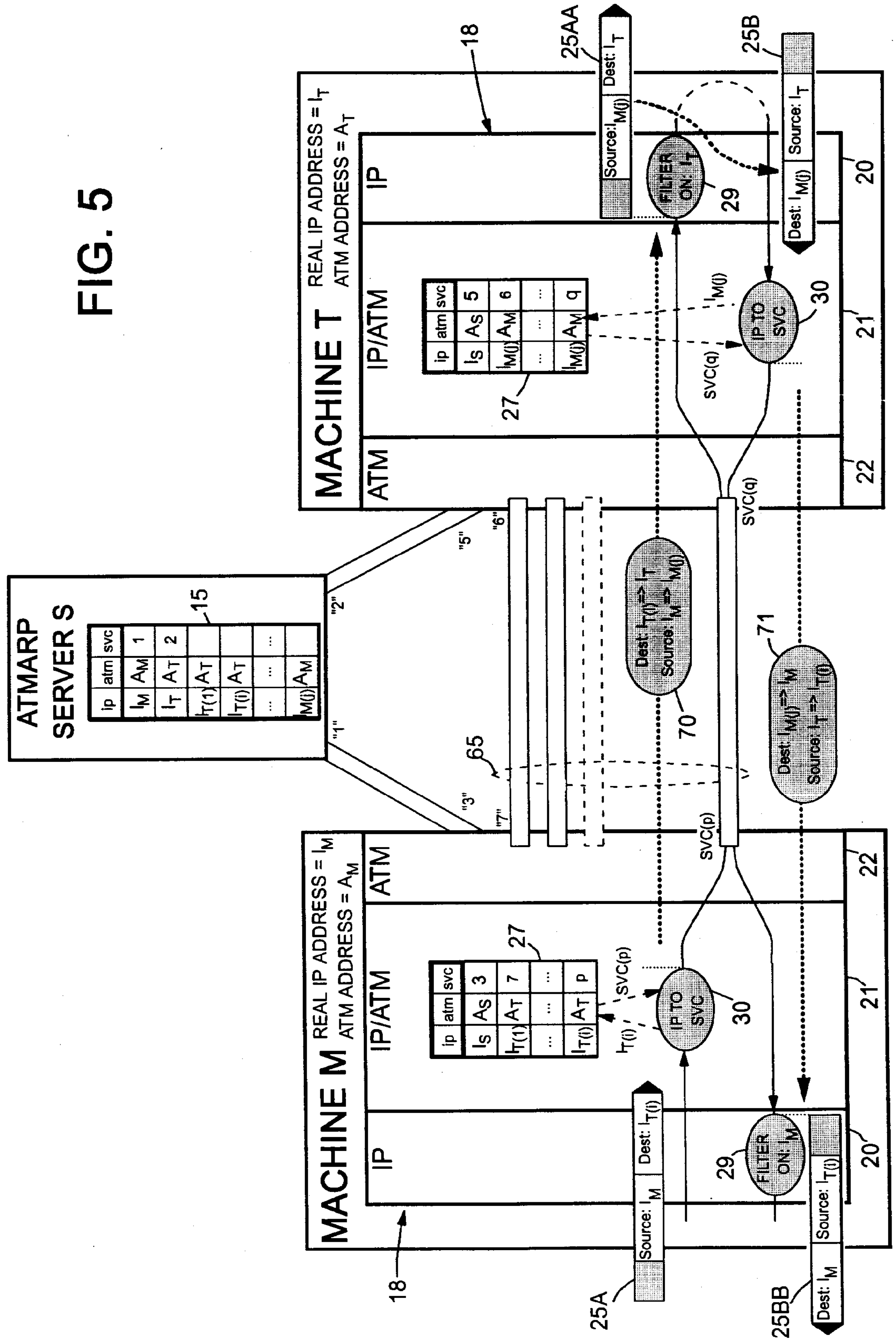


FIG. 5


MACHINE M
REAL IP ADDRESS = I_M
ATM ADDRESS = A_M
MACHINE T
REAL IP ADDRESS = I_T
ATM ADDRESS = A_T
ATMARP SERVER S
IP
IP/ATM
ATM
FILTER ON: I_M
FILTER ON: I_T
IP TO SVC
SVC(p)
SVC(q)
Source: I_M Dest: $I_{T(i)}$
Source: $I_{T(i)}$ Dest: I_M
Source: $I_{M(j)}$ Dest: I_T
Source: I_T Dest: $I_{M(j)}$
Dest: $I_{T(i)} \Rightarrow I_T$ Source: $I_M \Rightarrow I_{M(j)}$
Dest: $I_{M(j)} \Rightarrow I_M$ Source: $I_T \Rightarrow I_{T(i)}$
18
20
21
22
25A
25AA
25B
25BB
27
29
30
15
65
70
71

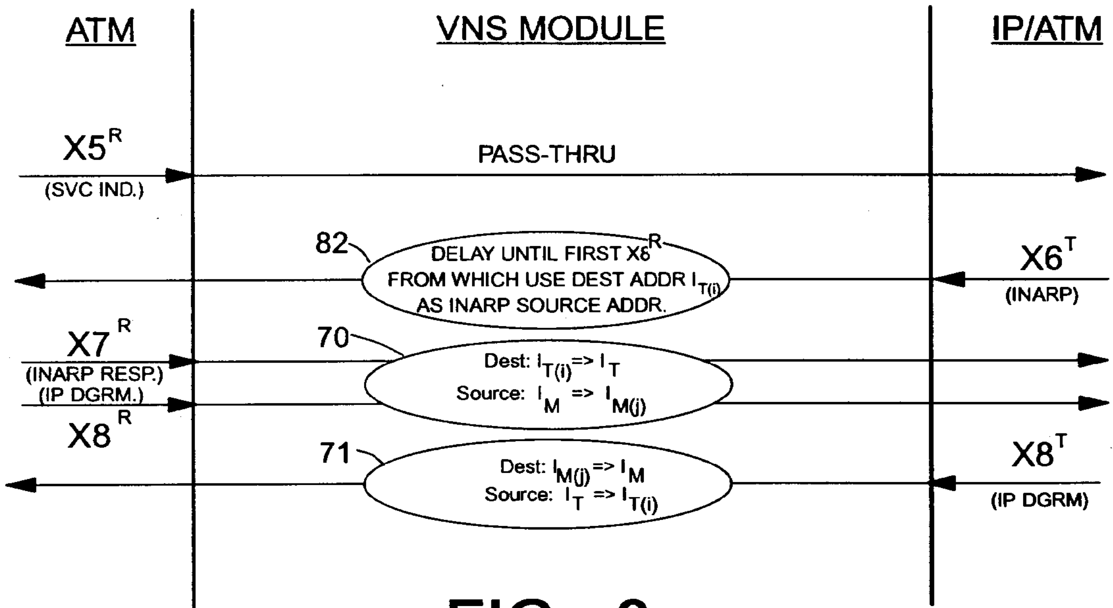

ATM
VNS MODULE
IP/ATM
X5R
(SVC IND.)
PASS-THRU
82
DELAY UNTIL FIRST X6R
FROM WHICH USE DEST ADDR IT(i)
AS INARP SOURCE ADDR.
X6T
(INARP)
X7R
(INARP RESP.)
(IP DGRM.)
X8R
70
Dest: IT(i) => IT
Source: IM => IM(j)
71
Dest: IM(j) => IM
Source: IT => IT(i)
X8T
(IP DGRM)

FIG. 6

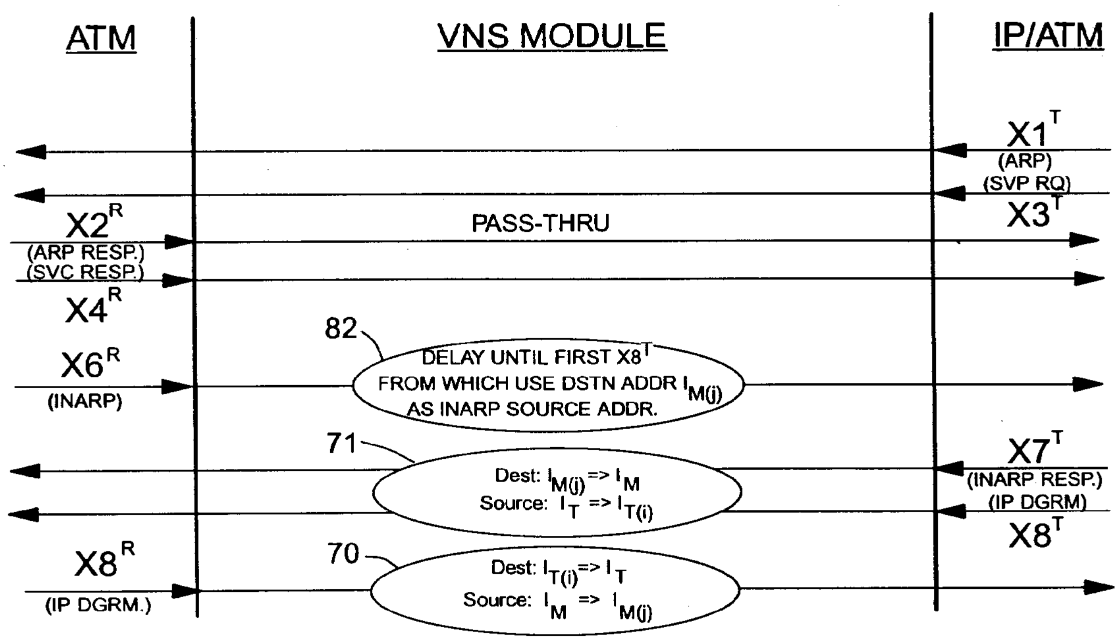

ATM
VNS MODULE
IP/ATM
X1T
(ARP)
(SVP RQ)
X3T
X2R
PASS-THRU
(ARP RESP.)
(SVC RESP.)
X4R
82
X6R
(INARP)
DELAY UNTIL FIRST X8T
FROM WHICH USE DSTN ADDR IM(j)
AS INARP SOURCE ADDR.
71
Dest: IM(j) => IM
Source: IT => IT(i)
X7T
(INARP RESP.)
(IP DGRM)
X8T
X8R
(IP DGRM.)
70
Dest: IT(i) => IT
Source: IM => IM(j)

FIG. 7

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 96 41 0106

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	COMPUTER COMMUNICATIONS REVIEW, vol. 25, no. 4, 1 October 1995, pages 49-58, XP000541650 PARULKAR G ET AL: "AITPM: A STRATEGY FOR INTEGRATING IP WITH ATM" * paragraph 2.1 * ---	1,10	H04L29/06 H04Q11/04
A	PROCEEDINGS OF THE ANNUAL SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIE, SANTA FE, NOV. 20 - 22, 1994, no. SYMP. 35, 20 November 1994, GOLDWASSER S (EDITOR), pages 424-434, XP000531950 LUND C ET AL: "IP OVER CONNECTION-ORIENTED NETWORKS AND DISTRIBUTIONAL PAGING" * paragraph 1 - paragraph 1.1 * ---	1,10	
A	DATA COMMUNICATIONS, vol. 24, no. 17, 1 December 1995, page 103/104, 106, 108, 110 XP000547618 MARSHALL G: "CLASSICAL IP OVER ARM:A STATUS REPORT" paragraph "Simple virtues"" ---	1,10,11	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L H04Q
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 35, no. 4A, 1 September 1992, pages 28-31, XP000314666 "COORDINATED ADDRESS RESOLUTION PROTOCOL PROCESSING" * the whole document * ---	6,8,9	
A	EP 0 523 386 A (FUJITSU) * page 4, line 20 - page 5, line 14; figure 3 * -----	12	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	13 March 1997	Staessen, B

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 July 2001 (12.07.2001)

PCT

(10) International Publication Number
WO 01/50688 A1

(51) International Patent Classification[7]: H04L 12/46, 12/56, 9/00

(21) International Application Number: PCT/SE00/02565

(22) International Filing Date: 18 December 2000 (18.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9904841-5 29 December 1999 (29.12.1999) SE

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ.) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventor: KRIENS, Peter; Finnasandsvägen 22, S-439 33 Onsala (SE).

(74) Agents: BERGENTALL, Annika et al.; Cegumark AB, P.O. Box 53047, S-400 14 Göteborg (SE).

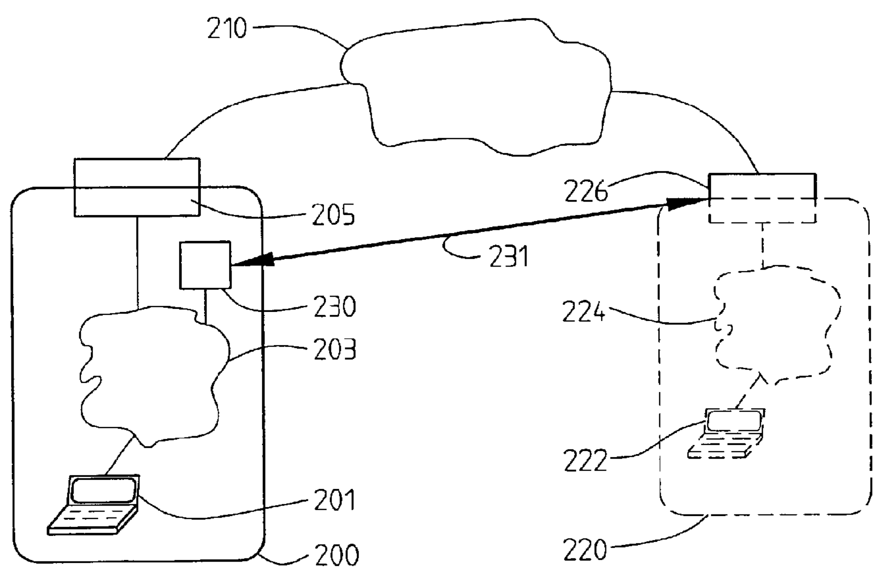
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR COMMUNICATION



(57) Abstract: A method and a system for establishing a connection between a first computer of a first computer network and a resource of a second computer network via a third network through a gateway intervening between the second computer network and the third network. A requester issues a request for a connection from the first computer to the resource by specifying a name of the resource. A temporary IP number is returned to the first computer in answer to the request. The temporary IP number is mapped to a tunnel to the gateway. The gateway administrates the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource and data packets arriving from the resource destined to the first computer, are routed through the tunnel to the first computer.

WO 01/50688 A1

Method and system for communication

FIELD OF THE INVENTION

The present invention relates generally to a method and a system for communicating between different networks, especially from one network to a host within a private network.

BACKGROUND TO THE INVENTION

The Internet is a collection of networks that can interwork. Clients connected to one network can access resources on other networks because data packets are routed from one network to the other. The Internet Protocol (IP) makes this possible. The same protocol can also be used to create private networks that are not directly connected to the Internet. These networks are called intranets. These intranets can be extended over a large area to remote offices using private lines. They are in a way the same intranet because there is a single authority that controls the network. Instead of private lines, an intranet can also be extended using the public internet as a tunneling medium. Instead of coupling an intranet directly to the Internet, the data traffic for a remote office is encapsulated and encrypted before being forwarded over the internet to the remote office. At the remote office, the reverse is done and the data package is placed in the local network. This is usually called a Virtual Private Network (VPN). For the end users it looks like a single private network, but the public Internet is used to securely transport data traffic between remote places.

In the Internet Protocol (IP) routing decisions are made on addresses. An address in IP is a 32-bit number. On the Internet, every host requires at least one unique number to be able to communicate. This unique number cannot be used by any other host on the Internet. A special official body allocates these IP numbers, and Internet routers all over the world must know how to map these IP numbers to the correct hosts. To simplify the routing and due to some original design choices the 4294967296 possible numbers are running out. For this reason there are a number of number ranges that are reserved which anybody can use privately in e.g. a private intranet. However, IP packets cannot be routed over the Internet with a number within these ranges, and consequently must remain within the private intranet. This creates a problem when users of such an intranet with host numbers in these number ranges want to access the Internet.

There are two basic very close solutions to this problem, one is the use of a firewall and the other is using network address translation (NAT). Using a firewall, all access to the Internet is terminated at a firewall computer that is connected both to the Internet and to the intranet. This firewall then looks at the access from the intranet and acts as a proxy to the Internet using its own public IP number that is valid on the internet. However, a proxy requires a program that knows about the protocol. The other solution using NAT has a computer acting as a gateway between the Internet and the intranet. Every packet directed to the Internet is processed by a program that replaces/translates the address and port of the packet, and keeps a track of on who's behalf this translation is done. If the return packet comes, the address is translated back to the original address. NAT is a very transparent solution but unfortunately has some problems with some protocols, which then requires special measures.

A user does not have to use IP numbers to address a packet. When a user uses a name as an address then a special application, a name server, is used to translate the name into an IP number. On the Internet the Domain Name System (DNS) is used for naming. This is a hierarchical scheme where a DNS server can provide the translation for a domain or it can look up the name via/in another name server. If a DNS server comprises tables for a domain, then it is authoritative for that domain. Each DNS server is registered in a parent DNS server, this is done recursively until the root DNS servers are reached. Private intranets also require special handling of the DNS. A host on the inside of the intranet should not be visible on the outside, i.e. on the Internet, because it has a private number. However, when NAT is used, hosts on the outside of the intranet are required to be present in the local intranet DNS. This is called a split universe DNS.

The real problems start when someone on the Internet wants private access to a host on an intranet with a private numbering scheme, or when two intranets with private numbering schemes want to connect privately. For example, assume that two companies, each with their own private intranet, decide to co-operate on a project and that they therefore want to share a number of resources on their respective intranets. This will cause a number of problems. The intranets cannot directly be routed to each other because the IP numbers used potentially overlap. Most probably the respective DNS of both companies are set-up as split universe DNSs and thus have no knowledge of each other's hosts. The normal forwarding to the internet DNS does not help since the domain of the other company does not expose the internal hosts with private IP numbers. Thus, since the internal hosts cannot see each other, it is impossible to route anything between them.

There have been a number of different solutions put forward. Unfortunately the known solutions either does not work for all protocols or they require complex administration or suffer from both disadvantages. For example, proxying is a solution to the problem. For each service that the companies want to share they have a publicly addressable host that contains a proxy for this service. This proxy does the mapping from the outside to the inside. A disadvantage of proxying is that it requires a significant amount of administration to set them up and then to keep them aligned with the original resources. Another disadvantage is that not all protocols are easy to proxy or have existing proxies. Another solution to the problem is to renumber the intranets so that a non-overlapping address space is created. A single DNS can then be used. However, this is a very complicated and heavy operation making it virtually impossible if the companies only co-operate on a project basis. This solution also requires a significant amount of trust between the parties in question.

A suggestion has also been disclosed in US patent number 5,898,830 to Wesinger, Jr. et al. (Wesinger). The Wesinger patent discloses a method of setting up virtual hosts in firewalls and using name based routing. The solution allegedly provides a full transparency for the users. However, this solution also only forwards hosts and not networks and it also requires quite a bit of administration.

There is thus a need to improve the methods of providing access to one or more hosts of a private intranet from the outside of the intranet with full transparency to users and a simple administration.

SUMMARY OF THE INVENTION

An object of the invention is to define a method and a system for transparently accessing hosts within a private intranet.

Another object of the invention is to define a method and a system for transparently accessing a host within private intranet by name.

A further object of the invention is to define a method and a system for accessing hosts within a private intranet with minimal administration.

A still further object of the invention is to define a method and a system for accessing hosts within a private intranet with security control and access control administration at the private intranet.

The aforementioned objects are achieved according to the invention by a method and a system for establishing a connection between a first computer of a first computer network and a resource, such as a second computer, of a second computer network via a third network through a gateway, such as a firewall, intervening between the second computer network and the third network. A requester issues a request for a connection from the first computer to the resource by specifying a name of the resource. A temporary IP number is returned to the first computer in answer to the request. The temporary IP number is mapped to a tunnel to the gateway. The gateway administrates the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource and data packets arriving from the resource destined to the first computer, are routed through the tunnel to the first computer.

The aforementioned objects are also achieved according to the invention by a method of establishing a connection between a first computer of a first computer network and a resource of a second computer network via a third network. The connection is established along a route through an intermediate system having an interface to the first computer network, and through a gateway intervening between the second computer network and the third network. The resource belongs to the domain of the gateway. According to the invention the method comprises a number of steps. A first step configuring the intermediate system with a tunnel from the intermediate system to the gateway. A second step mapping the tunnel with a requester and a domain name of the gateway. A third step wherein the requester issues a request for a connection from the first computer to the resource by specifying a name of the resource. A fourth step receiving the request at the intermediate system via the interface. A fifth step using a rule for matching the name of the resource with the gateway. A sixth step mapping the name of the resource to the tunnel. A seventh step returning a temporary IP number to the first computer in answer to the request. An eighth step mapping the temporary IP number to the name of the resource. A ninth step wherein the gateway administrates the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource. And a tenth step wherein the gateway administrating the handling of data packets such that data packets arriving from the resource destined to the first computer, are routed through the tunnel to the first computer via the intermediate system. It is to be understood that the steps according to the invention do not indicate any sequential execution, but is merely a manner to distinguish them.

The method can advantageously further comprise the step of transmitting a message with the mapping of the temporary IP number to the gateway by means of the tunnel.

Preferably the step of the gateway administrating the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource, comprises the substep of directing the intermediate system to translate source addresses of data packets addressed to the temporary IP number to be sent through the tunnel. The step of the gateway administrating the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource, can comprise the substep of directing the intermediate system to translate destination addresses of data packets addressed to the temporary IP number to be sent through the tunnel, by means of at least a partial DNS function in the intermediate system.

Advantageously the step of the gateway administrating the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource, can comprise the substep of the gateway translating source addresses of data packets arriving through the tunnel addressed to the temporary IP number and routing these data packets to the resource. The step of the gateway administrating the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource, can comprise the substep of the gateway translating destination addresses of data packets arriving through the tunnel addressed to the temporary IP number and routing these data packets to the resource. The step of the gateway administrating the handling of data packets such that data packets arriving from the resource destined to the first computer, are routed through the tunnel to the first computer via the intermediate system, can comprise the substep of the gateway translating source and destination addresses of data packets arriving from the resource destined to the first computer, and routing these data packets through the tunnel to the first computer via the intermediate system.

In some versions the step of the gateway administrating the handling of data packets such that data packets arriving from the resource destined to the first computer, are routed through the tunnel to the first computer via the intermediate system, can comprise the substep of directing the intermediate system to translate source and destination addresses of data packets arriving from the resource via the tunnel destined to the first computer.

In some versions the third network is a telecommunications network, in other versions it is the Internet, i.e. a computer network.

Advantageously the rule for matching the name of the resource with the gateway can be based on a mapping, and/or based on a list of hosts, and/or based on a regular or wildcard expression, and/or based on matching a domain name of the name of the resource with the domain name of the gateway.

Preferably the method further comprises the step of authenticating the requester at the first computer for access to the tunnel.

In some versions the name of the resource corresponds to a second computer within the second computer network, the second computer belonging to the domain of the gateway and comprising the resource. Then preferably the gateway administrates the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource residing on the second computer. Otherwise in other versions the gateway administrates the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource, the resource residing on a proxy of the second computer. Advantageously the proxy to which the gateway routes data packets addressed by the first computer to the temporary IP number, is in dependence on an identity of the requester.

One or more of the features of the above described different methods according to the invention can be combined in any desired manner, as long as the features are not contradictory.

The aforementioned objects are achieved in accordance with the invention also by a device arranged to establish a connection between a first computer of a first computer network and a resource of a second computer network via a third network. The connection being established along a route through the device having an interface to the first computer network, and through a gateway intervening between the second computer network and the third network. The resource belongs to the domain of the gateway. According to the invention the device comprises a number of means arranged to carry out the invention. A first means arranged to configure a tunnel from the device to the gateway. A second means arranged to map the tunnel with a requester and a domain name of the gateway. A third means arranged to receive a request, issued by the requester, via the interface for a connection from the first computer to the resource by specifying a name of the resource. A fourth means arranged to use a rule for matching the name of the resource with the gateway. A fifth means arranged to map the name of the resource to the tunnel. A sixth means arranged to return a temporary IP number to the first computer in answer to the request. A seventh means arranged to map the temporary IP number to the name of the resource. An eighth means arranged to cooperate with the gateway administrating the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel at the gateway, are routed to the resource. A ninth means arranged to cooperate with the gateway administrating the handling of data packets such that data packets arriving from the resource destined to the first computer, are at the gateway routed through the tunnel to the first computer via the device.

Different embodiments of the device according to the invention can be reached according to additional features mentioned above in connection with the description of the method according to the invention. The features of the above described different embodiments of a device according to the invention can be combined in any desired manner, as long as no conflict occurs.

By providing a device and a method for accessing one or more hosts within a private intranet, a plurality of advantages over prior art systems are obtained. According to the invention a route process/connection is made within a requesters network, which could also be a private intranet. Complete transparency is achieved; there is no restriction as to what protocol is used. The requester/user does not have to have any understanding of the set-up, such as the use of special ports or hosts and other network issues. The routing is name based; a requester/user requests access to a name of a host and will get an IP number in return to be used for access to the requested host. A requester is totally unaware that the request was intercepted and a route was set-up to respond to the IP number that was returned to the requester. All authentication and security issues such as access control can be handled by the private intranet to which access is desired. All the set-up at the requester's side that is required is some means of intercepting DNS requests before they are transferred to the internet. This means can, for example, be located in a gateway to the internet or at some other point logically before the gateway. This intercept means will have one or more tunnels configured to one or more private intranets and will determine if a DNS request is for one of the private intranets or not. If it determines that the DNS request is for one of the private intranets then a route process is set-up with an arbitrary but for the requestor valid IP number and a mapping to the corresponding tunnel is made. All access control can be handled at the other end of the tunnel, but in some embodiments some authentication and security is handled by the intercept means. Preferably all address translation is also done at the private intranet side of the tunnel, but in some embodiments at least some of the address translations can be handled directly by the intercept means, preferably under complete control of the private intranet side of the tunnel. Further advantages and variations of the invention will become apparent from the following.

DESCRIPTION OF THE FIGURES

The invention will now be described in more detail for explanatory, and in no sense limiting, purposes, with reference to the following figures, in which

Fig. 1	shows a diagram of communication situation to which the invention is suitable,
Fig. 2	shows a diagram of an implementation of the invention,
Fig. 3	shows a flow chart of an example of an intermediate system processing,
Fig. 4	shows a flow chart of an example of a firewall/gateway processing when receiving from a tunnel,
Fig. 5	shows a flow chart of an example of a firewall/gateway processing when transferring a data packet from a second computer to a first computer.

DESCRIPTION OF PREFERRED EMBODIMENTS

In order to clarify the system according to the invention, some examples of its use will now be described in connection with Figures 1 to 5.

Figure 1 shows a diagram of a communication situation to which the invention is suitable. A user/requestor which is situated at a first computer 101 connected to a first computer network 103, which network can comprise several computer networks, within a first domain 100, which can be open or private, desires to communicate/gain access to a second computer 122, a destination host, connected to a second computer network 124, which network can also comprise several networks, which in turn is within a second domain 120 which is private. A private domain is a domain which uses a private numbering scheme, i.e. hosts within the domain are not visible from the outside and can thus have the same number as a host on the internet. The first computer 101 and the second computer 122 are interconnected via, for example, an internet 110, a third computer network, a network, which will most likely comprise many networks, by means of a gateway/firewall 105 between the first computer network 103 and the third computer network 110, and a firewall/gateway 126 between the second computer network 124 and the third computer network 110. Other types of interconnections between the gateway/firewall 105 of the first computer network and the firewall/gateway 126 of the second computer network 124 are possible according to the invention. However, any direct ways of ordinary connection between the first computer 101 and the second computer 122 is not possible. The second computer 122 is not visible to the first computer 101 or to an internet 110, and if it is not visible then it is not ordinarily possible to route data packages from the first computer 101 to the second computer 122. Several known, less suitable, solutions to this situation have been discussed previously.

Figure 2 shows a diagram of an implementation of the invention. The set-up is the same as in figure 1 with a first computer 201, with a user/requestor, connected to a first computer network 203, which can comprise several computer networks, which in turn is connected to a gateway/firewall 205, all 201, 203, 205 of a first domain 200 which can be open or private. The gateway/firewall 205 is connected between the first computer network 203 and a third computer network 210. The third computer network 210, for example the Internet, will most likely comprise many networks. There is also a second computer 222, a desired destination, which is connected to a second computer network 224, which can comprise several networks, which in turn is connected to a firewall/gateway 226, all of a second domain 220 which is a private domain. The firewall/gateway 226 is connected between the third computer network 210 and the second computer network 224.

According to the invention there is also an intermediate system 230, an intercept means, connected somewhere into the first computer network 203. The intermediate system can be placed anywhere in the first domain 200, as long as it can intercept any DNS request from the first computer 201 before the request reaches the third computer network 210. To give a few examples, the intermediate system 230 can be a process running on the gateway/firewall 205, an intelligent connection box logically connected between the first computer 201 and the gateway/firewall 205, or even a process running on the first computer 201. The intermediate system 230 is preferably implemented as close as possible to, if not within, the gateway/firewall 205 to enable as many users/computers in the first domain 200 to have access to it, and thus have the possibilities of the invention. The intermediate system 230 will configure at least one tunnel 231 from the intermediate system to the firewall/gateway 226 of the second domain 220. A tunnel is a logical network connection between two processes, encapsulating the traffic during transport. Traffic over such a connection is traditionally encrypted to prevent eavesdropping. The tunnel or tunnels are preferably authenticated at regular, or irregular, intervals.

The intermediate system 230 will intercept DNS requests at least from the user or users and associate connection points/connected computers for which the intermediate system is set-up, in this example the first computer 201. The intermediate system must at least intercept DNS requests from the first computer 201 before the requests leave the domain 200. A user wanting a permitted access from the first computer 201 to the second computer 222 requests this by naming the second computer 222. The DNS request will then be intercepted by the intermediate system 230 which will determine if the requested name has any association with any tunnel 231 that is previously set-up. The determination can be based on a mapping, a list of hosts, or a regular or wildcard expression. In a preferred method the intermediate system 230 will try to match a domain name suffix of the second domain 220 to a domain name suffix of the DNS request for a match to the tunnel 231 of the example. As can be seen, the intermediate system does not have to be set-up with any details as to exactly which host or hosts are requested for within the second domain 220. If there is a match the intermediate system will set-up a route to the second domain 220 via a tunnel 231 in view of the match, in this case the described tunnel 231. An IP number, a temporary random IP number, will be generated/made and associated to the route. The generated/given temporary random IP number must at least be valid within the first domain 200 so that communication addressed to that temporary random IP number will be correctly routed to the associated tunnel 231 of the intermediate system 230. The first computer 201 will get the temporary random IP number back as an answer to its DNS request and then use this temporary random IP number for all communication to the second computer 222, at least during this session. The communication will end up at the route interface, which in turn will send it down the tunnel for correct routing to the desired destination, the second computer 222. The temporary random IP number is mapped to the complete name of the DNS request and sent as a message to the gateway/firewall 226 at the other end of the tunnel. The gateway/firewall 226 at the other end of the tunnel 231 will deal with all the details of routing packages to and from the correct desired host, in this case the second computer 222. Return communications will either have the correct destination, the first computer 201, when they emerge from the tunnel 231, or there has been some address translation in the intermediate system 230, governed by the gateway/firewall 226 of the second domain 220, in which case the intermediate system 230 will retranslate the communication so that it will be routed correctly within the first domain 200 to the first computer 201.

For an even better understanding of the invention, it will be explained in relation to flow diagrams of a specific implementation of the invention. Flow diagrams describe something as a string of events, one after another. The different processes according to the invention are mostly independent event-driven processes. The major difference is that the processes of the invention might not appear in the order described below, but it is believed that the flow diagrams can however provide an easier understanding of the invention.

Figure 3 shows a flow chart of an example of the processes of an intermediate system according to one specific implementation of the invention. In a first step 340 one or more predetermined tunnels are configured and tables/mappings are generated/set-up. A table can, for example, be set-up in a matrix where each line comprises; a user (optionally), a source IP number, a destination domain (e.g. *.ericsson.se), access time or times to the destination domain (optionally), a tunnel to the destination domain. The amount of information comprised in a table and the manner it is stored and mutually associated will vary in dependence of an implementation in question. A table/mapping can preferably be dynamically updated, i.e. information/entries added or deleted from for example a destination domain. In a second step 341 after the first step 340, authentication of the configured tunnel(s) and of configured users/requesters is done, for example, from which source IP number(s), e.g. the first computer, when, and to which domains access is allowed. In a third step 342 after the second step 341 it is determined if there is any communication to intercept or not, if there is none then it simply returns to itself. If there is some communication to intercept, the procedure continues with a fourth step 343 after the third step 342. The fourth step 343 determines if the communication was a DNS request or not. If the communication was determined to be a DNS request, then the procedure continues with a fifth step 344 after the fourth step 343. The fifth step 344 determines if the DNS request is from a configured user, e.g. the first computer, or not. If the DNS request is determined to have originated from a configured user then the procedure continues with a sixth step 345 after the fifth step 344. The sixth step 345 tries to match domains, in the configured user's map/table, with the domain of the DNS request. Thereafter the procedure continues with a seventh step 346 after the sixth step 345. The seventh step 346 determines if there is a match or not. If there is a match, then the procedure continues with an eighth step 347 after the seventh step 346. The eighth step 347 retrieves the entries of the user's map/table which correspond to the match of the seventh step 346 and also generates a temporary IP number, a temporary random IP number, which is a valid IP number in view of the place of the intermediate system. The intermediate system dynamically allocates a temporary IP number. Thereafter the procedure continues with a ninth step 348 after the eighth step 347. The ninth step 348 maps the temporary random IP number to a tunnel according to the retrieved entries in the user's map/table. Thereafter the procedure continues with a tenth step 349 after the ninth step 348. The tenth step 349 will send a message through the tunnel with a mapping of the temporary random IP number with the complete DNS request, i.e. the complete name of the desired destination, e.g. the second computer. Thereafter the procedure continues with an eleventh step 350 after the tenth step 349. The eleventh step 350 returns the temporary random IP number to the requester, e.g. the first computer, in answer to the DNS request.

If in the fourth step 343 it was determined that it was not a DNS request, then the procedure continues with a twelfth step 351 after the fourth step 343. The twelfth step determines if the communication is a data packet or not. If it is determined to be a data packet then the procedure continues with a thirteenth step 352 after the twelfth step 351. The thirteenth step 352 determines if the destination IP number of the data packet matches with any temporary random IP number which is mapped with the source IP number of the data packet. If there is a match, then the procedure continues with a fourteenth step 353 after the thirteenth step 352. The fourteenth step 353 sends the data packet in a tunnel according to the match and corresponding mapping/table entry. If it was determined in the twelfth step 351 that it was not a data packet, then the procedure continues with a fifteenth step 354 after the twelfth step 351. The fifteenth step 354 will ensure that the communication gets attention by means of some other processing. If it was determined in the thirteenth step 352 that there was no match, then the procedure continues with a sixteenth step 355 after the thirteenth step 352. The sixteenth step 355 provides normal routing of the data packet. If it was determined in the fifth step 344 that the DNS request was not from a configured user or if it was determined in the seventh step 346 that there is no match in the users domain name table, then the procedure continues with a seventeenth step 356 after the fifth step 344 or after the seventh step 346. The seventeenth step 356 provides a normal DNS request processing.

What happens next? We have opened a route interface process at the intermediate system and are now sending data packets and messages down a tunnel. Figure 4 shows a flow chart of an example of a second domain firewall/gateway processing when receiving from a tunnel. In a first step 460 the procedure waits for some communication received from a tunnel, and returns to itself as long as there is none. However when there is some communication received from a tunnel then the procedure continues with a second step 461 after the first step 460. The second step 461 determines if the communication is a message with a mapping of a temporary random IP number with a DNS request, or not, e.g a message sent by the tenth step 349 of Figure 3. If it determined that it is not a message with a mapping then the procedure continues with a third step 462 after the second step 461. The third step 462 determines if the communication is a data packet to be routed or not. If it is determined that it is a data packet to be routed then the procedure continues with a fourth step 463 after the third step 462. The fourth step 463 determines if there exists a mapping/table or not for the destination IP number, i.e. a temporary random IP number, of the data packet. If there exists a mapping/table for the destination IP number then the procedure continues with a fifth step 464 after the fourth step 463. The fifth step 464 determines if security control of the tunnel through which the communication came is OK and still valid. If it is determined that the security of the tunnel is satisfactory, then the procedure continues with a sixth step 465 after the fifth step 464. The sixth step 465 determines if, according to the table/map, the source IP number, e.g. the IP number of the first computer, of the data packet have allowed access to the destination IP number, i.e. the temporary random IP number, of the data packet. If it is determined that the data packet from the source IP number has access to the destination IP number then the procedure continues with a seventh step 466 after the sixth step 465. The seventh step 466 translates/re-maps the source IP number, e.g. the IP number of the first computer, to a temporary locally valid IP number, a temporary local IP number. This is done so that the packet can be routed properly in the second domain. After the seventh step 466 the procedure continues with an eighth step 467 which lookups the real local IP number of the destination, e.g. the second computer, by doing a DNS request in the second domain on the name received with the mapping to the temporary random IP number. The procedure then continues with a ninth step 468 after the eighth step 467. The ninth step 468 translates/re-maps the destination IP number, i.e. the temporary random IP number, of the data packet to the real local IP number of the destination, e.g. the second computer. Thereafter the procedure continues with a tenth step 469 after the ninth step 468. The tenth step 469 routes the data packet in the second domain to the destination, e.g. the second computer, with the real local IP number as destination and the temporary local IP number as the source.

If it was determined in the second step 461 that the communication was a map/table message then the procedure continues with an eleventh step 470 after the second step 461. The eleventh step 470 receives a mapping of a temporary random IP number with a DNS name, e.g. the second computer, of the second domain, and adds this to its mapping. If it was determined in the third step 462 that it was not a data packet to be routed that was received through the tunnel, then the procedure continues with a twelfth step 471 after the third step 462. The twelfth step 471 does other appropriate processing. If it was determined in the fifth step 464 that the security of the tunnel is not valid then the procedure could continue with a thirteenth step 472 after the fifth step 464. The thirteenth step 472 will then try to authenticate the tunnel, and then return and continue with the fifth step. If it was determined in the fourth step 463 that there does not exist a mapping/table or if it was determined in the sixth step 465 that the source IP number is not allowed access to the destination IP number, then the procedure continues with a fourteenth step 473 after either the fourth step 463 or the sixth step 465. The fourteenth will reject request, and not route the data packet, the "destination is unknown". Preferably security will also be alerted of an attempted breach of security.

As mentioned, packets must be able to be sent back to the original requester. Figure 5 shows a flow chart of an example of firewall/gateway processing when transferring a data packet from a second computer to a first computer. In a first step 580 it is checked if there is any communication from within the second computer network, and if not then just return to itself. If there is communication from within the second computer network, then the procedure continues with a second step 581 after the first step 580. The second step 581 determines if it is a data packet that should be routed. If it is a data packet to be routed then the procedure continues with a third step 582 after the second step 581. The third step 582 determines if the destination IP number of the data packet is equal to any valid temporary local IP number. If the destination IP number is matched then the procedure continues with a fourth step 583 after the third step 582. The fourth step retrieves the mapping/table that corresponds to the matched temporary local IP number to thereby find out where, which tunnel, to route the data package. After the fourth step 583 the procedure continues with a fifth step 584 which translates (re-maps) the source IP number, the IP number of the second computer, of the data packet to the temporary random IP number according to table (map). After the fifth step 584 the procedure continues with a sixth step 585 which translates (re-maps) the destination IP number, the temporary local IP number, of the data packet to the IP number of the first computer according to the table (map). Thereafter in a seventh step 586 after the sixth step 585 the data packet is transferred in an appropriate tunnel according to the table (map). If it was determined in the second step 581 that it is not a data packet that is to be routed then the procedure continues with an eighth step 587 after the second step 581 and does some other processing. If it was determined in the third step 582 that the destination IP number of the data packet is not equal to any valid temporary local IP number then the procedure continues with a ninth step 588 after the third step 582 and does a normal routing of the data packet.

The present invention can be put into apparatus-form either as pure hardware, as pure software or as a combination of both hardware and software. If the method according to the invention is realized in the form of software, it can be completely independent or it can be one part of a larger program. The software can suitably be located in a general-purpose computer or in a dedicated computer.

As a summary, the invention can basically be described as a method of accessing one or more hosts within a private network by means of a route interface process.

The invention is not limited to the embodiments described above but may be varied within the scope of the appended patent claims.

FIG 1	a diagram of communication situation to which the invention is suitable,
100	open or private first domain
101	user/requestor, a first computer,
103	a first computer network, can comprise several computer networks,
105	gateway/firewall between the first computer network and a third computer network,
110	internet, the third network, will most likely comprise many networks
120	private second domain,
122	a second computer, a destination,
124	a second computer network, can comprise several networks,
126	a firewall/gateway between the second computer network and the third computer network.

FIG 2	a diagram of an implementation of the invention,
200	open or private first domain,
201	user/requestor, a first computer, a source,
203	a first computer network, can comprise several computer networks,
205	gateway/firewall between the first computer network and a third computer network,
210	internet, the third computer network, will most likely comprise many networks,
220	private second domain,
222	a second computer, a destination,
224	a second computer network, can comprise several networks, to which the second computer is connected,
226	a firewall/gateway between the third computer network and the second computer network, the second computer,

230	an intermediate system between the third computer network and the first computer, the source,
231	a tunnel from the intermediate system to the firewall.
FIG 3	flow chart of an example of intermediate system processing,
340	: configure tunnels and generate tables/mappings
341	from 340: authentication of tunnel(s) and of users/requesters, for example from which source IP number(s), e.g. the first computer, when, and to which domains,
342	from 341 or no from itself: any communication ?
343	yes from 342: is it a DNS request ?
344	yes from 343: is it from a configured user, e.g. the first computer ?
345	yes from 344: try to match domains, in the configured user's table, with the domain of the DNS request,
346	from 345: is there a match,
347	yes from 346: get map/table and also generate a temporary IP number, a temporary random IP number, which is a valid IP number in view of the place of the intermediate system,
348	from 347: map the temporary IP number to a tunnel according to the retrieved map/table,
349	from 348: send message through tunnel with mapping of temporary random IP number with the DNS request,
350	from 349: return temporary random IP number to requester, e.g. the first computer, in answer to the DNS request,
351	no from 343: is it a data packet ?
352	yes from 351: does destination IP number of the data packet match with any temporary random IP number which is mapped with the source IP number of the data packet,
353	yes from 352: send data packet in a tunnel according to mapping/table entry,

354	no from 351: other processing,
355	no from 352: normal routing of data packet,
356	no from 344 or no from 346: do a normal DNS request processing.
FIG 4	flow chart of an example of firewall processing when receiving from a tunnel,
460	no from itself: communication received from a tunnel?
461	yes from 460: is the communication a map/table message?
462	no from 461: is the communication a data packet to be routed?
463	yes from 462: does there exist a mapping/table for the destination IP number, i.e. a temporary random IP number, of the data packet?
464	yes from 463 or from 472: security control of tunnel, through which the communication came, is it OK, still valid ?
465	yes from 464: does, according to the table/map, the source IP number, e.g. the IP number of the first computer, of the data packet have allowed access to the destination IP number, i.e. the temporary random IP number, of the data packet ?
466	yes from 465: translate/remap source IP number, e.g. the IP number of first computer, to a temporary locally valid IP number, a temporary local IP number,
467	from 466: lookup of real local IP number of destination, e.g. the second computer, by DNS in the second domain,
468	from 467: translate/remap destination IP number, i.e. the temporary random IP number, of the data packet to the real local IP number of the destination, e.g. the second computer,
469	from 468: route the data packet in the second domain to the destination, e.g. the second computer, with the real local IP number as destination and the temporary local IP number as the source,
470	yes from 461: receive a mapping of a temporary random IP number with a DNS name, e.g. the second computer, of the second domain,

471	no from 462: do other processing,
472	no from 464: authenticate tunnel,
473	no from 463 or no from 465: reject request, do not route data packet, "destination unknown", alarm security of an attempted break in.
FIG 5	flow chart of an example of firewall processing when transferring a data packet from a second computer to a first computer,
580	no from itself: communication from within the second computer network ?
581	yes from 580: is it a data packet that should be routed ?
582	yes from 581: is the destination IP number of the data packet equal any valid temporary local IP number ?
583	yes from 582: get mapping/table to find out where, which tunnel, to route the data package,
584	from 583: translate (remap) the source IP number, the IP number of the second computer, of the data packet to temporary random IP number according to table (map),
585	from 584: translate (remap) the destination IP number, the temporary local IP number, of the data packet to the IP number of the first computer according to the table (map),
586	from 585: transfer data packet in appropriate tunnel according to table (map)
587	no from 581: other processing,
588	no from 582: normal routing.

CLAIMS

1. A method of establishing a connection between a first computer of a first computer network and a resource of a second computer network via a third network, along a route through an intermediate system having an interface to the first computer network, and through a gateway intervening between the second computer network and the third network, the resource belonging to the domain of the gateway **characterized in that** the method comprises the following steps:

- configuring the intermediate system with a tunnel from the intermediate system to the gateway;
- mapping the tunnel with a requester and a domain name of the gateway;
- the requester issuing a request for a connection from the first computer to the resource by specifying a name of the resource;
- receiving the request at the intermediate system via the interface;
- using a rule for matching the name of the resource with the gateway;
- mapping the name of the resource to the tunnel;
- returning a temporary IP number to the first computer in answer to the request;
- mapping the temporary IP number to the name of the resource;
- the gateway administrating the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource;
- the gateway administrating the handling of data packets such that data packets arriving from the resource destined to the first computer, are routed through the tunnel to the first computer via the intermediate system.

2. The method according to claim 1, **characterized in that** the method further comprises the step of:

- transmitting a message with the mapping of the temporary IP number to the gateway by means of the tunnel.

3. The method according to claim 1 or 2, **characterized in that** the step of the gateway administrating the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource, comprises the substep of:

- directing the intermediate system to translate source addresses of data packets addressed to the temporary IP number to be sent through the tunnel.

4. The method according to any one of claims 1 to 3, **characterized in that** the step of the gateway administrating the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource, comprises the substep of:

- directing the intermediate system to translate destination addresses of data packets addressed to the temporary IP number to be sent through the tunnel, by means of at least a partial DNS function in the intermediate system.

5. The method according to claim 1 or 2, **characterized in that** the step of the gateway administrating the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource, comprises the substep of:

- the gateway translating source addresses of data packets arriving through the tunnel addressed to the temporary IP number and routing these data packets to the resource.

6. The method according to claim 1, 2, 3 or 5, **characterized in that** the step of the gateway administrating the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource, comprises the substep of:

- the gateway translating destination addresses of data packets arriving through the tunnel addressed to the temporary IP number and routing these data packets to the resource.

7. The method according to any one of claims 1 to 6, **characterized in that** the step of the gateway administrating the handling of data packets such that data packets arriving from the resource destined to the first computer, are routed through the tunnel to the first computer via the intermediate system, comprises the substep of:

- the gateway translating source and destination addresses of data packets arriving from the resource destined to the first computer, and routing these data packets through the tunnel to the first computer via the intermediate system.

8. The method according to any one of claims 1 to 6, **characterized in that** the step of the gateway administrating the handling of data packets such that data packets arriving from the resource destined to the first computer, are routed through the tunnel to the first computer via the intermediate system, comprises the substep of:

- directing the intermediate system to translate source and destination addresses of data packets arriving from the resource via the tunnel destined to the first computer.

9. The method according to any one of claims 1 to 8, **characterized in that** the third network is a telecommunications network.

10. The method according to any one of claims 1 to 8, **characterized in that** the third network is the Internet.

11. The method according to any one of claims 1 to 10, **characterized in that** the rule for matching the name of the resource with the gateway is based on a mapping.

12. The method according to any one of claims 1 to 10, **characterized in that** the rule for matching the name of the resource with the gateway is based on a list of hosts.

13. The method according to any one of claims 1 to 10, **characterized in that** the rule for matching the name of the resource with the gateway is based on a regular or wildcard expression.

14. The method according to any one of claims 1 to 10, **characterized in that** the rule for matching the name of the resource with the gateway is based on matching a domain name of the name of the resource with the domain name of the gateway.

15. The method according to any one of claims 1 to 14, **characterized in that** the method further comprises the step of:

- authenticating the requester at the first computer for access to the tunnel.

16. The method according to any one of claims 1 to 15, **characterized in that** the name of the resource corresponds to a second computer within the second computer network, the second computer belonging to the domain of the gateway and comprising the resource.

17. The method according to claim 16, **characterized in that** the gateway administrating the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource residing on the second computer.

18. The method according to claim 16, **characterized in that** the gateway administrating the handling of data packets such that data packets addressed by

the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource, the resource residing on a proxy of the second computer.

19. The method according to claim 18, **characterized in that** the proxy to which the gateway routes data packets addressed by the first computer to the temporary IP number, is in dependence on an identity of the requester.

20. A device arranged to establish a connection between a first computer of a first computer network and a resource of a second computer network via a third network, along a route through the device having an interface to the first computer network, and through a gateway intervening between the second computer network and the third network, the resource belonging to the domain of the gateway **characterized in that** the device comprises:

- means arranged to configure a tunnel from the device to the gateway,
- means arranged to map the tunnel with a requester and a domain name of the gateway,
- means arranged to receive a request, issued by the requester, via the interface for a connection from the first computer to the resource by specifying a name of the resource,
- means arranged to use a rule for matching the name of the resource with the gateway,
- means arranged to map the name of the resource to the tunnel,
- means arranged to return a temporary IP number to the first computer in answer to the request,
- means arranged to map the temporary IP number to the name of the resource,
- means arranged to cooperate with the gateway administrating the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel at the gateway, are routed to the resource,

- means arranged to cooperate with the gateway administrating the handling of data packets such that data packets arriving from the resource destined to the first computer, are at the gateway routed through the tunnel to the first computer via the device.

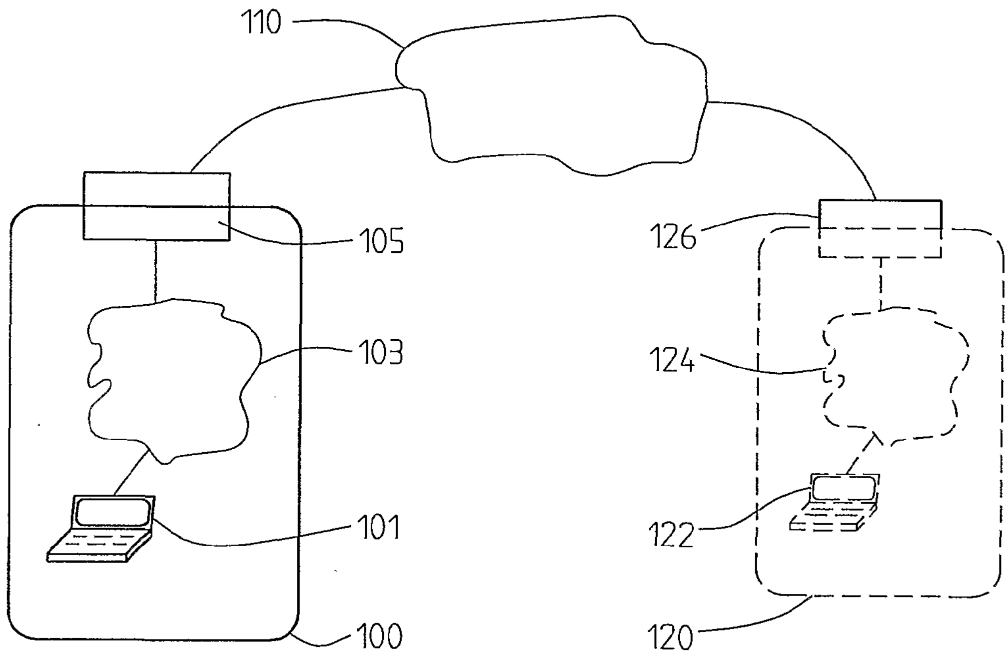

110
105
103
101
100
126
124
122
120

Fig. 1

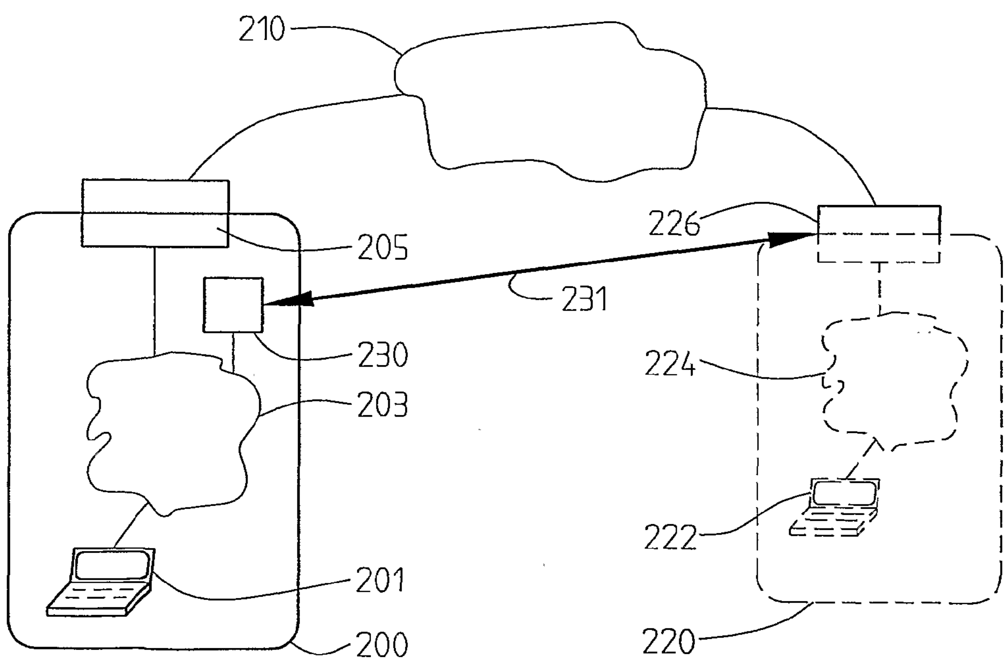

210
205
230
203
201
200
226
231
224
222
220

Fig. 2

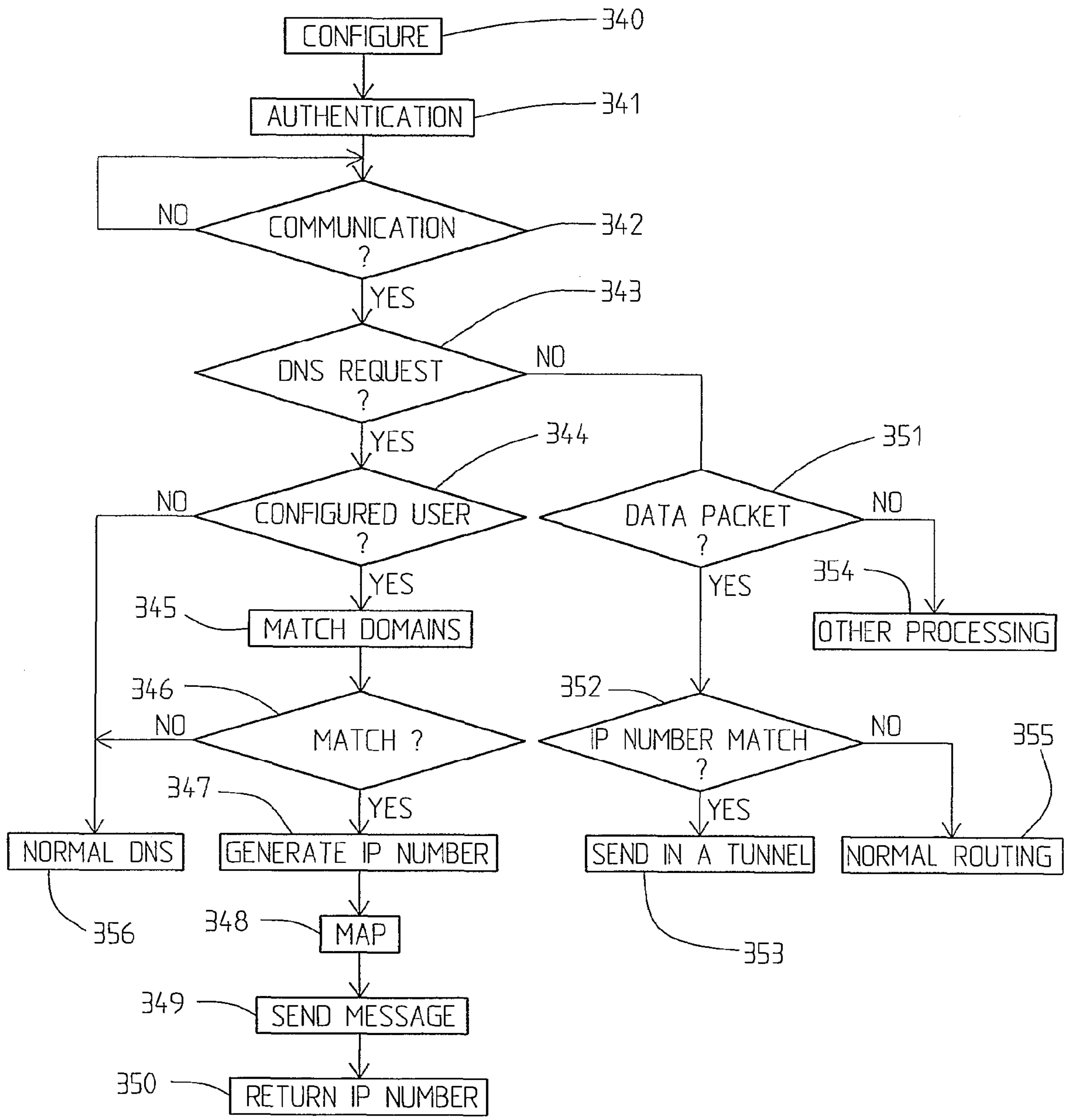

CONFIGURE
340
AUTHENTICATION
341
COMMUNICATION ?
NO
YES
342
DNS REQUEST ?
NO
YES
343
CONFIGURED USER ?
NO
YES
344
DATA PACKET ?
NO
YES
351
354
OTHER PROCESSING
345
MATCH DOMAINS
346
MATCH ?
NO
YES
352
IP NUMBER MATCH ?
NO
YES
355
347
NORMAL DNS
GENERATE IP NUMBER
SEND IN A TUNNEL
NORMAL ROUTING
356
348
MAP
353
349
SEND MESSAGE
350
RETURN IP NUMBER

Fig. 3

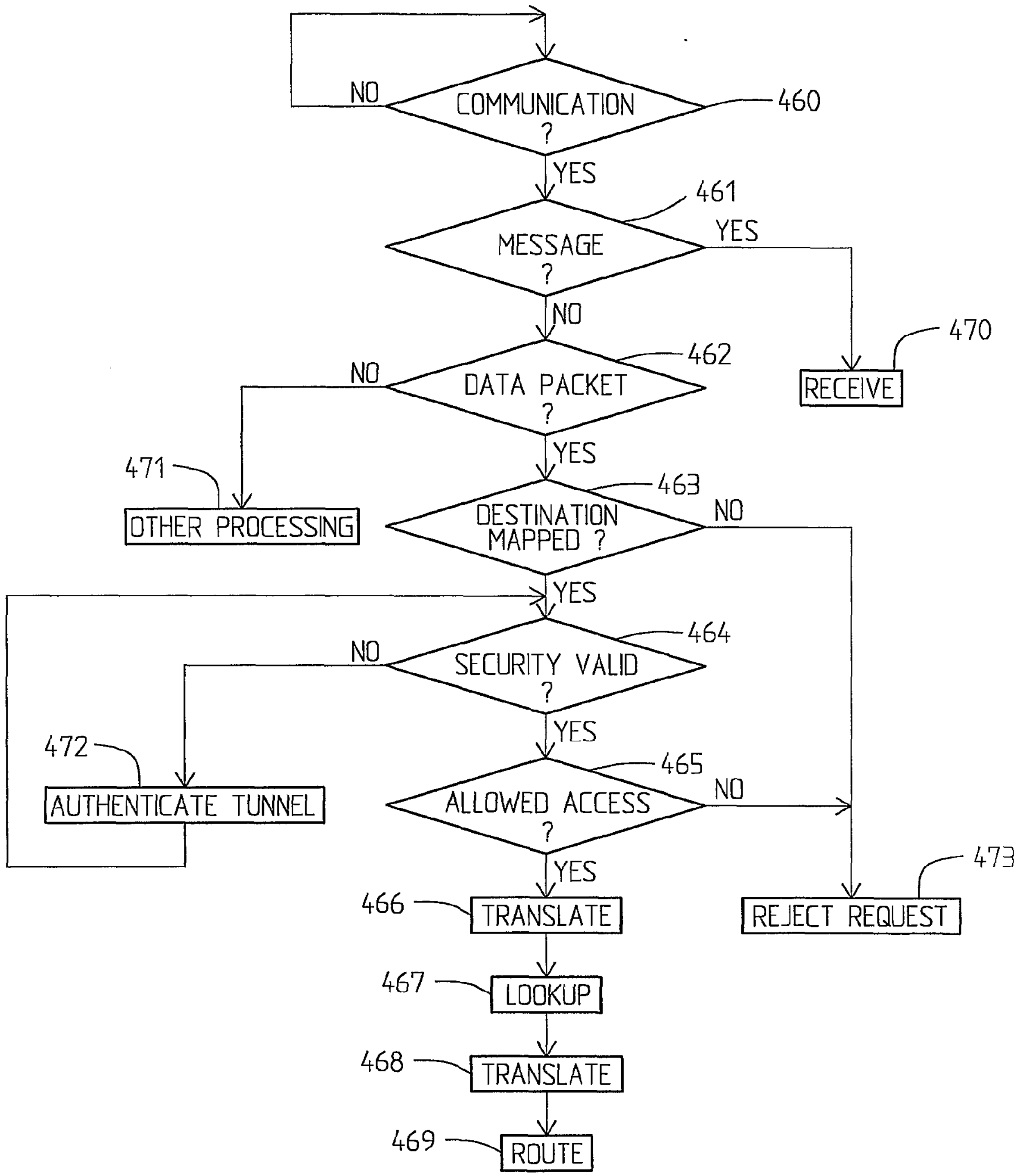

COMMUNICATION ?
NO
YES
460
MESSAGE ?
461
YES
NO
RECEIVE
470
DATA PACKET ?
462
NO
YES
OTHER PROCESSING
471
DESTINATION MAPPED ?
463
NO
YES
SECURITY VALID ?
464
NO
YES
AUTHENTICATE TUNNEL
472
ALLOWED ACCESS ?
465
NO
YES
REJECT REQUEST
473
TRANSLATE
466
LOOKUP
467
TRANSLATE
468
ROUTE
469

Fig. 4

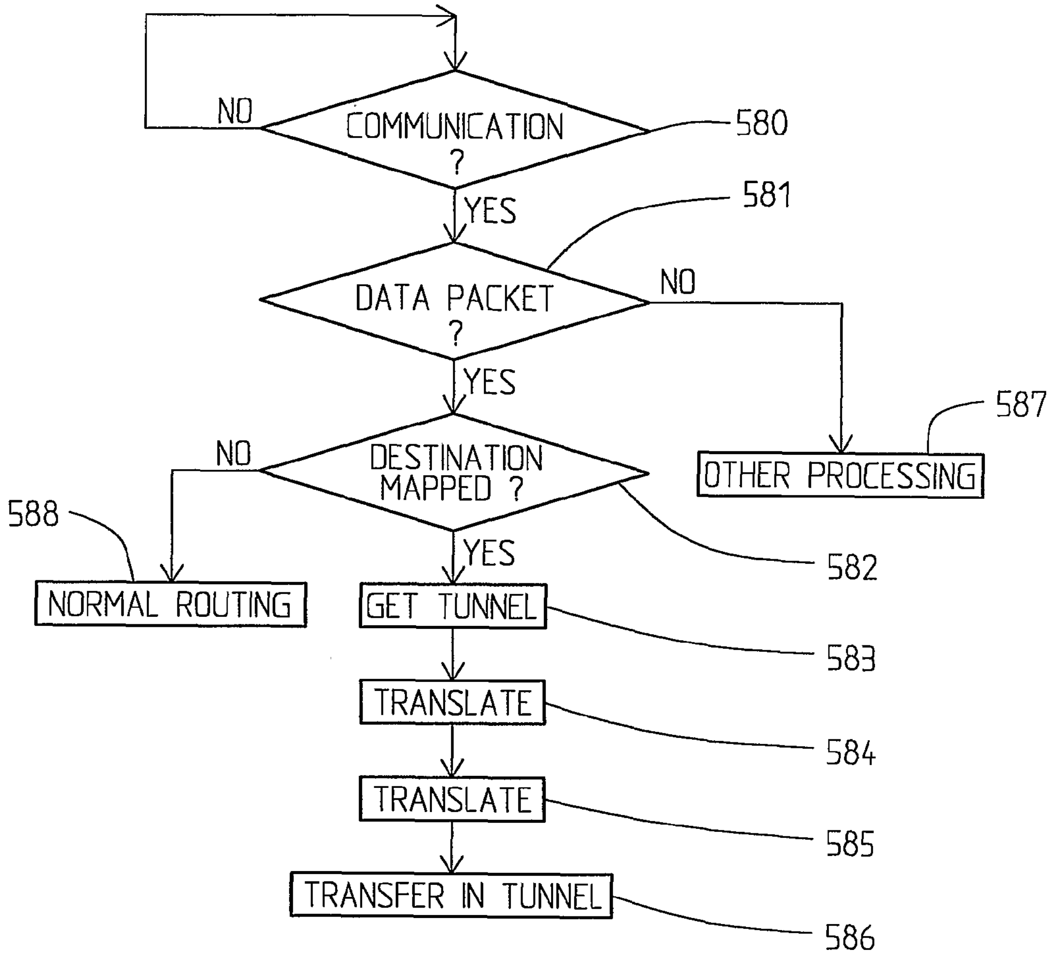

COMMUNICATION ?
NO
580
YES
DATA PACKET ?
581
NO
YES
DESTINATION MAPPED ?
NO
587
OTHER PROCESSING
588
582
YES
NORMAL ROUTING
GET TUNNEL
583
TRANSLATE
584
TRANSLATE
585
TRANSFER IN TUNNEL
586

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/02565

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 12/46, H04L 12/56, H04L 9/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, G09F, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5898830 A (R.E.WESINGER, JR. ET AL), 27 April 1999 (27.04.99), column 3, line 47 - column 4, line 52, figure 1, claims 1-10, abstract, cited in Application --	1-20
A	C. HUITEMA: An Experiment in DNS BasedIP Routing. K B Labs Kashpureff Boling Laboratories, Inc., Network Working Group, rfc 1383, INRIA dec. 1992. http:www.kblabs.com/lab/lib/rfcs/1300/rfc1383.txt.html --	1-20
A	WO 9859470 A2 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)), 30 December 1998 (30.12.98), page 1, line 13 - page 3, line 16, figures 1-2, claims 1-12 --	1,20

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 April 2001	18 -04- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Roger Bou Faisal/LR Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/02565

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9726731 A1 (RAPTOR SYSTEMS, INC.), 24 July 1997 (24.07.97), see whole document	1,20

--

INTERNATIONAL SEARCH REPORT
Information on patent family members

25/02/01

International application No.
PCT/SE 00/02565

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5898830 A	27/04/99	US 6052788 A	18/04/00
WO 9859470 A2	30/12/98	AU 8052398 A	04/01/99
		SE 9702385 A	24/12/98
WO 9726731 A1	24/07/97	AU 2242697 A	11/08/97

Form PCT/ISA/210 (patent family annex) (July 1998)

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification [6] **:**
G06F 12/14, 1/00

A1

(11) International Publication Number: **WO 98/55930**

(43) International Publication Date: 10 December 1998 (10.12.98)

(21) International Application Number: PCT/IB98/00578

(22) International Filing Date: 20 April 1998 (20.04.98)

(30) Priority Data:
97201667.9 3 June 1997 (03.06.97) EP
(34) Countries for which the regional or international application was filed: NL et al.

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL–5621 BA Eindhoven (NL).

(71) Applicant *(for SE only)*: PHILIPS AB [SE/SE]; Kottbygatan 7, Kista, S–164 85 Stockholm (SE).

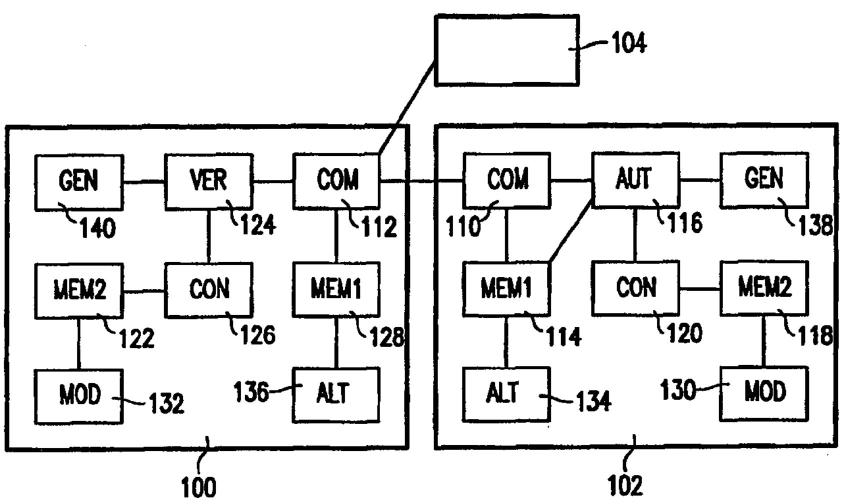
(72) Inventor: TANG, Wei–Jin; Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL).

(74) Agent: GROENENDAAL, Antonius, W., M.; Internationaal Octrooibureau B.V., P.O. Box 220, NL–5600 AE Eindhoven (NL).

(81) Designated States: JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: AUTHENTICATION SYSTEM



(57) Abstract

The authentication system comprises at least one station (102) and a host (104). The station (102) comprises a memory (118) for electronically storing a plurality of authentication items. Constructing means (120) are used to construct an authentication control element, such as a key, from a part of the authentication items which is selected for each message. Authentication means (116) authenticate the message substantially uniquely under control of the authentication control element constructed for the message. The authenticated message is sent to the host. The host comprises a memory (122) for electronically storing the authentication items of the station. The host comprises constructing means (126) for constructing for each received authenticated message an authentication control element in the same way as the station. Verification means (124) are used for, under control of the authentication control element, verifying the authenticity of the received message.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

Authentication system.

The invention relates to an authentication system comprising at least one station and a host; the station comprising: authentication means for, based upon an authentication algorithm, authenticating a message; and communication means for sending the authenticated message to the host; the host comprising: communication means for receiving an authenticated message; and verification means for verifying the authenticity of the received message by checking the received message with an authentication algorithm corresponding to a station which sent the message.

With the increase of electronic communication and electronic financial transactions, identification and authentication has become an essential aspect of many systems. Normally in an authenticated transaction three parties are involved: a host, a station and a user of the station. The host may, for example, be a central computer at a bank, at a retailer, or at a company providing services via Internet, or be a file server. The station may be a personal computer (PC), a Personal Digital Assistant (PDA) or a hand-held PC (HPC), usually connected or connectable via telecommunications to the host computer. The message may be a digital representation of a user generated message, including an instruction to a bank, but may also be computer data or computer code, such as a Java applet. In many applications, the station is split into two parts: a user station and an access station.

An identification, such as a communication address, which uniquely identifies the station is stored in the memory of the station. A message generated in the station, usually at the request of the user, is authenticated using an authentication algorithm. Typically, the message is authenticated by generating an additional digital signature. The authenticated message is sent to the host together with the identification of the station. The host uses the same or a complementary authentication algorithm to verify the authenticity of the message.

For certain applications, like a user instructing a bank to transfer money from a bank account, it may be required that the station performs some form of access control ensuring that only an authorised user can issue the instruction. The access control may, for instance, be based on a PIN-code or password. Also more advanced methods, for instance based on biometrical information, may be used. The access information may be passed on to the host as part of the message. For other applications, like a transfer of a small amount of electronic money, it may not be required or, in view of privacy or safety, even be undesired that additional access control is performed or that the access information is transferred to the host. The access control is not part of the invention.

Most authentication algorithms are based on encryption algorithms, such as the symmetrical DES algorithm or the asymmetrical public-key RSA algorithm. Typically, the same algorithm is used for each station and a dedicated key is used to make the algorithm act in a manner specific for the station. The security provided by such algorithms is mainly based in the algorithmic strength of the involved algorithms, which are, as a consequence, complicated and costly to implement, which is a particular drawback for simple consumer electronic products.

It is an object of the invention to provide an authentication system of the kind set forth, which is simple to develop. It is a further object to provide such a system which can be cost-effectively implemented in consumer electronic products. It is a further object to provide such an authentication system which offers a high level of security.

To achieve this object, the authentication system according to the invention is characterised in that the station comprises a memory for electronically storing a plurality of authentication items; the host comprises a memory for electronically storing the authentication items of the station in association with an identification of the station;

the station comprises constructing means for constructing for each message a corresponding authentication control element; the constructing means being operable to select for the message a part of the plurality of authentication items and to construct the authentication control element from the selected part, where the authentication control element in practical circumstances causes the authentication algorithm to substantially authenticate the corresponding message uniquely; and

the host comprises constructing means for constructing for each received authenticated message an authentication control element from the authentication items associated with a station which sent the message; the construction being the same as performed by the associated station.

The system according to the invention is based on the insight that the simple manner in which parents and children identify each other when they are not in direct contact, such as in the case of a kidnapping, can form the basis of an automatic authentication system. If for instance a child is kidnapped, the parents want to be sure that the kidnappers indeed hold the child and that, for instance, a ransom demand genuinely relates to their child. At the moment when identification of, for instance, the child is required, the child informs the kidnappers of a few events from a large set of events known to the child and parents and unknown to others (or at least to the kidnappers). For each communication with the kidnappers, the parents may request that the child recalls other events. This ensures that the kidnappers have to keep the child alive. It also ensures that no fraudulent kidnappers, who in one way or another intercepted a set of identifying events, can re-use this set for authenticating a fraudulent demand.

Based on this insight, the host (parent) and the station (child) share a large set of authentication items. For each message which needs to be authenticated, a small sub-set from the authentication items is selected and used to form an authentication control element which controls an authentication algorithm. In practical circumstances the authentication algorithm authenticates with a high likelihood the corresponding message uniquely under control of the authentication control element. A main strength of the system according to the invention lies in unpredictably authenticating messages by selecting a subset of authentication items from a relatively large set, where for each next message other items may be selected. This allows the use of a simple authentication algorithm, where the emphasis is not on the algorithmic strength of the algorithm, such as the difficulty of predicting for a message the corresponding authenticated message, but on using the algorithm in an unpredictable manner. A correlation which might occur in the authentications generated for successive messages can be broken by using an authentication control element, which is not related to the authentication algorithm. The authentication items, which determine the authentication control element can be generated in advance using sophisticated means, such as real random sequence generators, if desired. For a fraudulent party to be able to break the system, the fraudulent party needs not only to intercept sufficient messages to be able to break the authentication algorithm but also to determine the entire set of authentication items. The size of the set of authentication items and the size of the subset used to generate an authentication control element can be chosen to optimally suit the application in which the system is used. As an example, for a not very demanding application, a set of authentication items formed by a couple of hundred random bytes may be used, where the authentication algorithm may be based on a substitution, using a substitution table. Some or all elements of the substitution table which have been used during the substitution are replaced by new elements derived from the random bytes. These new elements form the authentication control element. The new elements may, for instance, be selected using a (pseudo-)random number generator. For more demanding applications, more authentication items may be used. If desired, also the complexity of the involved algorithm may be increased, for instance by basing the authentication algorithm on algorithmically strong encryption algorithms, such as DES, where the authentication control element forms a key for DES. For applications which require a high level of security, the authentication items and the algorithms are preferably stored in, respectively, executed in a secure module, such as a tamper-proof IC.

It should be noted that the Dutch Giro (Postbank) uses the TAN (Transaction Number) system for electronic payments by customers using a PC and a modem. The customers of the Postbank receive via regular mail several transaction numbers printed on a piece of paper. For each transaction the client has to enter a next transaction number until all numbers have been used, at which moment the client receives a new set of numbers. A fraudulent party has, in general, easy access to the transaction numbers at the customers premises. Furthermore, the distribution of the transaction numbers from the host to the customer makes the system vulnerable for fraudulent parties intercepting the list.

For simple systems, for instance used to check the authenticity of an entry ticket to a sporting event or concert, it may be sufficient to differentiate between authentic and non-authentic stations. The station, such as an electronic ticket, may be re-used for authenticating a series of events by using an event-specific message. For a more demanding system, such as involving financial transactions, a message is advantageously authenticated in a manner unique for the station.

The measure as defined in the dependent claim 2 has the advantage that the uniqueness of the station identification is used for authenticating a message in a manner unique for the station. The station identification, which is used to distinguish the station amongst the other stations of the system with respect to the host, may, for instance, be a communication address or an account number.

The measure as defined in the dependent claim 3 has the advantage that a fraudulent party needs to intercept messages for each station in order to determine the authentication items specific for the station, making the task of the fraudulent party more complicated.

The measure as defined in the dependent claim 4 has the advantage that the set of shared information (the authentication item) is updated as the station and the host experience more shared events, like authenticating a message. In this way a fraudulent party not only has to determine the set of authentication items but also how the items are modified over time.

In a further embodiment of the system according to the invention, the system is characterised in that the modification means is operative to modify an authentication item at least partly based on an event independent of the authentication items. In this way it becomes even more important for a fraudulent party to intercept and record all messages in order to be able to determine the authentication items. In a simple form the modification may be (partly) based on the previously authenticated message(s). This has the advantage that the message is already transferred to the host allowing the host to perform the same modification. In some systems the content of the message may be too predictable to significantly increase the task of a fraudulent party in breaking the authentication. In such systems more unpredictable events, such as the time at which the last message was authenticated, may be used. To allow the host to perform the same modification, the event has to be informed to the host, for instance, in the form of a time-stamp. Preferably, the modification is at least partly based a random or pseudo-random event. Advantageously, the least-significant bits of a clock are used, giving for most systems a sufficiently random event, particularly if messages are authenticated individually and not processed in a sequential batch.

The measure as defined in the dependent claim 6 has the advantage that it becomes more difficult for a fraudulent party to collect messages relating to the same station. The identification may, for instance, be a conventional communication identification, such as a communication address or a telephone number. Instead of in addition to such a communication identification, the station identification may also be based on an identification, such as an indication of an account number, which is chosen independent of the communication identification. For such a combined identification only part of the identification, e.g. only the account number, may be modified, whereas the other part remains fixed. Preferably, the host locates information, such as the authentication items, used for verifying the authentication at least partially based on the variable part of the identification. As an example, the host may locate the relevant information for verifying a message in dependence on a bank account number. Instead of using the real bank account number as the identification (and exchanging the real bank account number), a virtual bank account number is used. The station and the host are initially loaded with the same virtual account number. The host also knows how to associate (map) the virtual number with the real bank account number. Usually, the station also knows the real bank account number for local operations, such as display to the user, and preferably hides the virtual number from the user. The virtual number is exchanged and not the real number. Only in exceptional cases, e.g. when the synchronisation in updating the virtual number is lost between the host and the station, it may be required to re-synchronise to a new virtual number using the real number for once as an identification. Both the station and the host can alter the virtual number in the same way, keeping the real underlying bank account number fixed (i.e. only the mapping between a variable virtual number and a fixed real number is changed). In such a scenario, the virtual number acts as the identification according to the invention. Particularly, for mobile stations, such as a PDA or a smart-card, with no fixed communication link to the host, it becomes practically impossible for a fraudulent party to collect messages related to a specific station or a specific application within the station, such as an application for financial transfers/information retrieval, downloading of software or playing of a network game, where each application uses an application-specific authentication algorithm or set of authentication items. This allows the use of less authentication items or a simpler authentication algorithm. It further allows to detect fraudulent messages in an early stage. As an example, in a system where no more than 65,000 stations need to distinguished (implying that in principle a two-byte identification would be sufficient) a larger identification of, for instance, four of six bytes may be used, where the identification is chosen dynamically. If a four-byte identification is used, the host can identify almost all received fraudulent messages as being fraudulent simply by checking the identification. Only for in average 1 out of 65,000 fraudulent messages the authentication of the message (which typically involves more processing) needs to be checked. This makes the system suitable for use in environments, such as Internet, where brute-force attacks by generating many different fraudulent messages may occur. Preferably, the response time of the host is similar regardless of the station identification being valid or not, ensuring that fraudulent parties can not distinguish between valid and invalid station identifications. Advantageously, the alteration means alters the station identification at least partly based on a message and/or a time-stamp. In this way it becomes even more important for a fraudulent party to intercept and record all messages in order to be able to determine the current station identification.

The measure as defined in the dependent claim 7 has the advantage that in a simple way it can be ensured that messages, even the same messages, are with a high likelihood authenticated differently. Furthermore, it limits the possibilities of a fraudulent party, including the legitimate owner or designer of the station, to generate known messages and from the corresponding authenticated message derive the authentication items of the station.

The measure as defined in the dependent claim 8 has the advantage that the host independently generates the same additional data, providing a further check of the authenticity of the message.

The measure as defined in the dependent claim 9 has the advantage that by incorporating the additional data into the message, for instance by mixing the additional data with the message, and authenticating the resulting message, the host only needs to verify the resulting message as before and can then discard the additional data, without being able to generate the additional data. Advantageously, each station generates the additional data in a manner unique for the station.

The measure as defined in the dependent claim 10 has the advantage that by using a state variable, such as a feedback state for a random number generator, the construction means can autonomously select different parts of the authentication items for a large sequence of messages. Preferably any periodicity in the selection is sufficiently large in view of the application. By ensuring that the selection also depends on the authentication items (for instance on a subset of the authentication items), which have been generated independent of the construction means, a correlation which might occur in successive selections can be reduced. As an example, the control vector could be one authentication item which is XOR-ed over the basic output, such as a random number, of the construction means. The control vector itself may be each time randomly selected from the set of authentication items.

These and other aspects of the invention will be apparent from and elucidated with reference to the embodiments shown in the drawings.

Fig. 1 shows a block diagram of a system according to the invention,

Fig 2 shows a flow-chart of a possible operation in the station 102, and

Fig. 3 shows a flow diagram of a basic operation which can be used in steps of Fig. 2.

Fig. 1 shows a block diagram of a system according to the invention. The authentication system comprises a host 100 and at least one station. As an example two stations 102 and 104 are shown. Further details of the stations will be given with reference to station 102 only. Typically, the host 100 is implemented on a computer suitable for acting as a server. The station may be implemented on, for instance, a Personal Computer (PC), a Personal Digital Assistant (PDA) or a hand-held PC (HPC). In an exemplary application, a user instructs a bank to perform a financial transaction. The user enters the instruction in his station. The station generates a corresponding message, authenticates the message and transfers the message to the host computer at the bank. The host checks the authentication and, if valid, proceeds with processing the instruction. The authentication serves various well-known purposes, such as reducing the chance of a third party, pretending to be another party, transmitting a message on behalf of the other party (the third party may have generated the fraudulent message or may be a re-transmitting an intercepted message which has been validly transmitted by the original party) and reducing the chance of the original party repudiating the message. The system may also be used for various other forms of electronic communication, such as for authenticating electronic mail, the exchange of electronic documents (such as an HTML document) or program modules (such as Java applets), or the communication between software objects located in different computers. If the receiving party can trust the sending party, the authentication ensures that the receiving party can safely use the received digital data, without having any risk of, for instance, having received virus-infected data or data which may adversely effect the local station (e.g. by discarding locally stored data). Particularly in situations where stations do not share prior knowledge and wish to safely communicate, the communication preferably takes place via a trusted party. With respect to the sending station the trusted party acts like a host according to the invention and the sending station acts like a station according to the invention. With respect to the receiving station the trusted party acts like a station according to the invention and the receiving station acts like a host according to the invention. The trusted party relays a message received from a sending station to a receiving station if the trusted party has successfully verified the authenticity of the received message, using a verification procedure matching the authentication procedure of the sending station. The trusted party authenticates the received message, using a procedure agreed with the receiving station, before transmitting the message to the receiving station.

It will be understood that, particularly for mobile applications, the station 102 may be split into, for instance, a user station and an access station. The access station establishes the communication with the host 100 and may, for instance, be fixedly located in a shop, a petrol station or integrated with an automatic teller machine of a bank. The access station may also be located at the premises of the user and, for instance, be integrated with a personal computer or audio/video set-top box. The user station ensures a station-specific authentication. The user station may, for instance, be formed by a PDA communicating via IrDA to another PDA or personal computer acting as an access station. As another example, the user station may be formed by a smart-card, where the access station includes a smart-card reader.

The station 102 and the host computer 100 can communicate digitally. To this end, the station comprises communication means 110 for digitally communicating with the host 100. Similarly, the host 100 comprises communication means 112 for digital communication with the station. Usually, the communication will take place using telecommunication, either wired or wireless. The communication means 110 and 112 may be formed by a conventional modem, operated under control of the processor of the station or, respectively, the host. The communication may also be based on local communication, such as a Local Area Network (LAN), infra-red communication or local RF communication, such as for instance used in walkie-talkies. Conventional hardware/software, such as a LAN interface and driver software, may be used for implementing locally operating communication means 110 and 112.

Using the communication facilities, digital data can be exchanged between the station and the host. Typically, the exchange is bi-directional. In certain simple systems, it may be sufficient if communication is only possible from the station to the host. The station 102 comprises a memory 114 for electronically storing a station identification, which uniquely identifies the station to the host. The identification may take several forms. For instance the identification may be an identification at communication level, such as a communication address or a telephone number. The identification may also take the form of an account number, which may also be used in combination with a communication identification. For each communication session, the identification of the station 102 is transferred to the host 100, allowing the host 100 to correlate data exchanged during the session to the identified station 102. It will be appreciated that in certain circumstances, such as where the station is fixedly connected to the host, the identification may be implicit (e.g. which port the station is connected to).

The station 102 comprises authentication means 116 for authenticating a message. As described above, the message may, for instance, be a digital representation of a user generated message, including an instruction to a bank, but may also be computer data or computer code, such as a Java applet, or messages generated by computers (e.g. for playing a multi-user game on several computers). The authentication is based upon an authentication algorithm. In principle the authentication algorithm may be chosen to suit the security requirements of the application. Many techniques for authenticating a message are known. One way is to use a symmetrical encryption algorithm like DES, where the station and the host share the same private key. The station encrypts the message using the key and transmits the encrypted message to the host, along with the station identification. The host uses the station identification to retrieve the key corresponding to the station and uses this key to decrypt the message. Various schemes, such as encryption feedback, message counters or time-stamps, may be used to ensure that the same message is authenticated differently, eliminating the possibility of intercepting and re-transmitting the same message, which then would be accepted again as a valid message by the host. In situations where it is preferred that the entire message (or part of it) is readable, the message may be transmitted in addition to the encrypted message. In such a case, the host can also verify the authenticity of the received data by encrypting the received plain message and comparing it to the received encrypted message. To reduce the length of the data to be transmitted, the authentication part may also be smaller. It is well-known that this can be achieved by using a one-way hash function and encrypting the resulting hash value. The algorithm itself may simple and based on basic techniques, like confusion and diffusion. Using a confusion technique, such as substitution, the relationship between the plain text and the cipher text is obscured. For high security applications, it may be preferred to use a substitution scheme which operates on blocks of more than one letter. Using a diffusion technique, such as a transposition (also called permutation), the redundancy of the plain text is spread out over the cipher text. It is preferred that linear operations are used in combination with at least one non-linear operation. Whatever authentication algorithm is used, for the system according to the invention it is assumed that the algorithm is used under control of a so-called authentication control element. For an authentication algorithm using DES, this could be the private key. For an authentication algorithm based on substitution this may be (part of) a substitution table. For an authentication algorithm based on a permutation this may be (part of) a permutation matrix. In general, using a different authentication control element will with a high likelihood cause the authentication algorithm to authenticate a same message differently. For most algorithms it will hold that if the same authentication control element is used, the same messages will be authenticated in the same way. However, some authentication algorithms may have measures, such as an internal feedback, ensuring that this is not the case. For such algorithms, the authentication control element can, for instance, play the role of an initial seed, where the algorithm is (at least partly) reset each time a new authentication control element is provided, or the authentication control element may act as a supplementary control vector, which is, for instance, combined with the internal state variable or to the output of the algorithm. The combination may, for instance, take the form of an XOR operation or an operation in $GF(2^8)$ for byte-oriented algorithms. Depending on the algorithm, the authentication control element may be regarded as data or more as an operation.

According to the invention, the station 102 electronically stores a plurality of authentication items in a memory 118. It will be appreciated that the memories 114 and 118 may be combined. The station further comprises constructing means 120 for constructing the authentication control element. The construction means 120 derives the authentication control element from a small part of the entire set of authentication items. This may be done in various ways, like randomly selecting some items or some bits of some items and using the selected parts directly or after a mixing operation as the authentication control element. For each message a corresponding authentication control element is constructed. The authentication items are independent of the authentication algorithm, and as a consequence also the authentication control element is independent of the authentication algorithm. In this way any correlation which might occur when the authentication algorithm were to be used for authenticating a sequence of messages under control of the same authentication control element is broken by the unrelated authentication control element. It will be understood that the size of a small part with respect to the entire set of authentication items has to be determined in view of the requirements of the application in which the system is used and in view of further improvements as described below for further embodiments. In systems where the set of authentication items is highly static, a small part may correspond to a few percent or less of the entire set. In a system where the set is highly dynamic (i.e. regularly updated), a small part may be over 50% of the current set of authentication items, where the selected part is small compared to the superset of authentication items formed by the current authentication items and future changed authentication items. Such a higher percentage can particularly be used if the influence of an update of authentication items is spread over substantially all authentication items of an involved set of authentication items. Preferably, the authentication items have been generated randomly or selected randomly from a very large set of suitable authentication items. For instance, for a system used for financial transactions the authentication items may be generated in a secure manner using a high quality (real-)random sequence generator located at secure premises of a bank. The authentication items are loaded into the memory 118 of the station 102. The host 100 electronically stores a copy of the authentication items of the station in a memory 122. It will be appreciated that, depending on the authentication algorithm, the authentication item may be a data element, such as a bit or a byte, or an operation, such as a byte-wise XOR or a $GF(2^8)$ multiplication.

The authentication control element in practical circumstances causes the authentication algorithm with a high likelihood to authenticate the corresponding message uniquely. For high demanding systems, preferably each authentication control element is derived from at least one authentication item which has not been used before. Such a new authentication item may be combined with (e.g. mixed in with) authentication items which have been used before. In less demanding systems, a same selection of authentication items may be used a number of times for constructing an authentication control element. The construction means 120 should be such that even then the authentication control elements are different.

The host 100 comprises verification means 124 for verifying the authenticity of the received message. The verification means 124 checks the received message with an authentication algorithm which corresponds to the algorithm used by the station which send the message. The algorithm may be the same for all stations. If more than one algorithm is used, the host can locate the algorithm based on the received station identification. To this end, the station identification may be stored in a memory 128 of the host. It will be appreciated that the host may perform the verification by using the same authentication algorithm as used by the station to generate an authentication from the message and checks whether this matches the received authentication. For certain algorithms, the host may need to use an inverse algorithm of the algorithm used by the station. The host 100 comprises constructing means 126 for constructing for each received authenticated message an authentication control element from the authentication items for the identified station in a same manner as the station identified for the message.

In a further embodiment, the authentication algorithm authenticates each message in a manner unique for the station. This may be achieved by making the message authentication dependent on the station identification, which is unique for the station. Such a dependency may be obtained by deriving a key of the authentication algorithm or the authentication control element (partly) from the station identification.

Preferably, the authentication is made unique for the station by using authentication items which are unique for the station. The host 100 associates the copy of the authentication items of the station with the station, for instance, by combining the memories 122 and 128 and storing the station identification together with the authentication items. The construction means 126 of the host uses the received station identification to locate a matching station identification in memory 128 and via the matching identification locate the authentication items in memory 122 corresponding to the station.

In a further embodiment, the station 102 comprises modification means 130 for modifying at least one of the authentication items after the authenticating means has authenticated a message. The host comprises modification means 132 for modifying at least one of the authentication items for the station in the same way as the modification means 130 of the station. Preferably, the station 102 effectuates the modification after the station has received a confirmation from the host 100 that the host has successfully received the message and verified the authentication of the message. It is preferred that any confirmation message is also authenticated in a manner similar to a message transferred from the station to the host. The modification means 132 performs the modification if the verification means 124 has successfully verified an authenticated message received from the station. Also, additional transaction and roll-back mechanisms as used for distributed databases may be used to ensure that the station 102 and the host 100 remain synchronised. The modification may take place in any suitable form. One way would be to combine a selection of other authentication items to one new authentication item and to replace an existing authentication item with the new item. Preferably, the modification means 130, 132 is operative to modify an authentication item at least partly based on an event independent of the authentication items. Advantageously, the modification is based on the content of one or more of the preceding messages. As an alternative or in combination, the modification may also be based on a time-stamp of one or more of the preceding messages. If a time-stamp is used, the time-stamp is also transferred to the host 100. The host 100 and the station 102 may also share an algorithm for generating or collecting the same random data elements, where information exchanged between the station 102 and the host 100 determines which of the random data elements is used for generating the new authentication item.

In a further embodiment, the station 102 comprises alteration means 134 for altering the station identification after the authenticating means 116 has authenticated a message. The host 100 comprises alteration means 136 for altering the station identification for the station in the same way as the station after the verification means 124 has successfully verified a received authenticated message. Preferably, as described for generating the authentication control element, the altering is performed under control of a set of authentication items, which are independent of the altering algorithm. For instance, a selection of the authentication items may be 'mixed-in' with the station identification to obtain a new station identification. Preferably, a separate set of authentication items is used for generating the station identifications. Similarly as described for the modification means 130, the alteration means 134, 136 may alter the station identification at least partly based on a message and/or a time-stamp. This may, for instance, be achieved by modifying the set of authentication items used for generating the station identifications. The identification associated with the station may be a communication identification, such as a communication address or a telephone number, which is also used for the communication hardware/software to transfer messages between the desired devices. Preferably, the identification is a higher level identification, which is independent of the communication identification. An example of such a higher level identification is a bank account number. Both types of identification may also be used in combination. For such a combination, the communication identification may be kept the same whereas the higher level identification may be altered. If an identification, such as a virtual bank account number representing a real bank account number, is changed the underlying item (e.g. the real bank account number) is preferably kept the same, implying that in the host only the mapping of the representation (virtual number) to the actual underlying item is changed. Particularly, if the station interfaces to the user using the real underlying item, also the mapping in the station is updated. In some systems it may not be required that the station is aware of the real underlying item. It will be appreciated that a station (and as a consequence also the host) may have several different identifications, e.g. several bank account numbers, associated with the station, where each identification corresponds to its own unique set of authentication items. In order to exchange messages with several hosts, preferably the station has several identifications (at least one for each host) with corresponding set of authentication items.

In a further embodiment, the station 102 comprises data generation means 138 for generating additional data. The authentication means 116 is operative to authenticate a message in dependence on the additional data. The generated additional data is such that in practical circumstances with a high likelihood the additional data is different for each message. The additional data may be used in various ways. One way is to use the additional data in a manner 'invisible' to the outside world, except to the host 100. This can, for instance, be achieved, by first concatenating the original message and the additional data. Next, the authentication of the message with the additional data is determined, followed by removing the additional data before transferring the authenticated message (i.e. the original message plus the authentication for both the original message and the additional data) to the host 100. In this scenario, the host 100 also comprises data generation means 140 for generating additional data for a received authenticated message in a same manner as the identified station. The verification means 124 is operative to verify the authenticity of the received authenticated message in dependence on the additional data. The verification may be done similar to the authentication by first adding the additional data before checking the authentication. If the use of additional data is optional, it is preferred that the station 102 informs the host 100 whether the option is used for a message or not. This can be achieved by using an additional field, of for instance only one bit, in the message.

As an alternative to using the 'invisible' additional data, the authentication means 116 may also incorporate the additional data into the message before authenticating the message. In this scenario the additional data is not removed from the message by the station 102. The additional data may be simply concatenated to or may be mixed in with the original message. The verification means 124 verifies the authentication of the entire message (original message plus the additional data). For the purpose of verification, the entire message can be regarded as the message. After the verification, the additional data is removed and the original message is passed on for further processing. The removal may be straightforward, particularly if the additional data is simply concatenated. For a more complex mix operation, the host 100 may need to perform a same mixing operation as the station in order to be able to determine at which positions in the message the data elements of the additional data are located or an inverse mixing operation to be able to remove the additional data from the message.

It will be appreciated that also a combination of using 'visible' and 'invisible' additional data can be advantageously used. In such a combination, for instance, the station 102 and the host 100 share some information A. The station 102 generates an additional part B and uses both parts A and B to generate additional data. The authentication is based on the entire additional data. The station 102 transfers in combination with the message the additional data as well as the additional part B to the host 100. The host 100 generates in the same way the additional data using the received part B and the part A, which was already stored in the host 100. The host 100 checks whether the generated additional data matches the received additional data. If so, the authenticity of the data is checked further. Particularly if the additional data and the parts A and B are relatively small compared to the message, this provides an effective filter for the host 100 for fraudulent messages without requiring a full verification of the entire message.

In a further embodiment, the construction means 120 and 126 comprise at least one state variable which influences the construction of the authentication control element. The construction means 120 and 126 update the state variable at least each time a message has been authenticated. The use of a state variable allows the construction means to autonomously select different parts of the authentication items for a large sequence of messages. The construction means may, for instance, be based on a (pseudo-)random sequence generator, where the state variable corresponds to a feedback state of the generator. Preferably, any periodicity in the sequence is sufficiently large in view of the application. For instance, the periodicity is larger than the expected number of messages authenticated by the station 102. The state variable may also be a pointer to an authentication item (in the set of authentication items), which has been last used for generating the authentication control element. If more than one authentication items is used for constructing the authentication control element, a separate state variable may be used for all of them. The construction means 120 and 126 construct the authentication control element under control of a control vector. The control vector may directly influence the operation of the construction means 120, 126, or, alternatively, may influence the output of the construction means 120,126 in a different manner, for instance by XOR-ing the control vector over the basic output (e.g. random number) of the construction means 120,126. The control vector is derived from a selection of the authentication items, for instance by 'randomly' selecting an authentication item from a given set of authentication items and using the selected item as the control vector. Preferably a separate set of authentication items are used for forming the control vector. Like described earlier, these authentication items may also be modified.

Fig. 2 shows a flow-chart of a possible operation in the station 102. In step 200, the station collects information regarding the identification of the user of the station, such as a user name and password, or a fingerprint. In step 202 the identification is checked. If not accepted, the previous steps are repeated one or more times, if required with a time delay and a limit on the number of retries. (Preferably, the station 102 reports a failed attempt when the legitimate owner successfully gains access). If accepted, in step 204 information is collected from the user based on which a message is compiled. Next, in step 206 it is checked whether additional data is required. If so, in step 208 the additional data is generated and added (for instance appended) in step 210 to the message. In step 212 it is checked whether the message needs to be scrambled. If so, the scrambling occurs in step 213. The scrambling may be restricted to the original message generated at step 204 or may cover the entire message created at step 210. In step 214 the authentication for the message is generated and added to the message (e.g. appended) in step 216. In step 218 it is checked whether the option of dynamically changing the station identification is used. If so, in step

220 a new station identification is created. In both cases, in step 222 the station identification is added (e.g. prefixed) to the message. In step 224, one or more of the authentication items are changed. Preferably, authentication items which have been involved in any of the preceding steps are modified. Finally, in step 226 the message is sent to the host 100. Steps may be added to ensure that the host 100 and the station 102 stay synchronised (i.e. that authentication items and shared state variables are updated synchronously). In the exceptional case that the synchronisation in updating the virtual number used as the station identification is lost between the host and the station, it may be required to re-synchronise to a new virtual number by once using the real number as an identification. It will be appreciated that a similar corresponding flow-chart can be used to describe the activities of the host 100.

Fig. 3 shows a flow diagram of a basic operation which can be used in various steps of Fig. 2. The core operation is performed in block 300, where a (pseudo-)random number is generated. In block 302 a seed for the generator is selected from a first set of authentication items. A correlation which might occur in the sequence of generated numbers is broken by using a feedback and combining in block 304 the feedback with at least one authentication item. The combination may simply be an XOR operation. The authentication item is selected in block 306 from a second set of authentication items. It will be appreciated that the combination may also be in the output path 308 of the generator 304 instead of in the feedback path. The sets of authentication items may, for instance, consist of 100 authentication items each. The actual number is preferably chosen to optimally suit the need of the application. The selection performed in blocks 302 and 306 may be straightforward, like each time selecting a next one of the authentication items. Using such a scheme, preferably the first authentication items have been changed, by the time all authentication items have been used. The basic operation of Fig. 3 may be used directly to generate the additional data of step 208 or the new station identification of step 220 in Fig. 2. For the scrambling of step 214, the random numbers can be used as entries in a substitution matrix. For instance, assuming that the data elements of a message are bytes, a substitution table may be used with 256 entries each with a byte value, where each byte value specifies a substitution value for a data element with a value matching the entry number in the table. Alternatively, the substitution byte may be selected based on the position of the byte in the original message, if desired, in combination with the value of the byte in the original message. As an example, a pointer which (logically) points to an element in the substitution matrix is loaded with an initial offset. This offset may be selected using the basic operation of Fig. 3. The value of the first byte of the message is combined with the pointer value (e.g. added to it). The value of the element in the substitution matrix to which the pointer points at that moment is chosen as the substitution value. For the next byte of the message, similarly the value of the next byte of the message is combined with the then valid pointer value, etc.. The pointer may be one-dimensional, where the substitution matrix is logically arranged as a sequence where each row follows the previous row to form a long row (alternatively the columns may be logically concatenated). Such arrangement usually matches the physical arrangement for storing a matrix in a memory. Using a suitable modulo operation the pointer can be kept within the desired range of, in the example, 256 matrix elements. It will be appreciated that instead of a one dimensional pointer also a separate row and column index may be used. Instead of using the pointer or index value directly for selecting the substitution element, the value may also be fed through a randomiser, such as a random sequence generator, whose output is used as a pointer into the substitution table. In these examples it is assumed that the output of the generation 300 is a byte value. If not, a conversion may be required. The random numbers may also be used to create a permutation matrix for permuting the positions of data elements in the message. The basic operation can also be used for changing an authentication item in step 224. Since the changing, preferably, also depends on an external event, additional information, such as a message, and/or a time-stamp and/or a message counter, is fed into the random number generator 300. The output of the generator 300 may directly replace a constituent element (e.g. a value) of an authentication item.

For generating the authentication in step 214 of Fig. 2, a similar routine as described for the substitution may be used. In such a routine, in one round one data element (one signature element) is selected from a matrix (or long row) with data elements. Preferably, the initial data elements of the matrix have been generated randomly, where the data elements are refreshed by using the output of basic operation of Fig. 3 as a new data element (preferably in combination with a historical influence, such as the content of a previous message or a time-stamp, as described before). Alternatively, the output of the basic operation may be used to randomly shuffle the data elements of the matrix. A pointer which (logically) points to an element in the matrix is loaded with an initial offset. This offset may be selected using the basic operation of Fig. 3, which is preferably used under control of different sets of authentication items as used for generating the elements of the matrix. The value of the first byte of the message is combined with the pointer value (e.g. added to it). Next, the value of the next byte of the message is combined with the then valid pointer value, etc.. When all bytes of the message have been processed, the value of the element in the matrix to which the pointer points at that moment is chosen as the signature value. The security can be improved by repeating the routine to generate further signature values. Preferably, for each successive round of generating a signature value a different initial offset value is chosen. Alternatively, a subsequent rounds continues using the last obtained pointer value of the previous as the starting value for the new round.

It will be appreciated that, although the description focuses on the communication from the station 102 to the host 100, the same authentication items can also be used for communication from the host 100 to the station 102.

CLAIMS

1. An authentication system comprising at least one station and a host;

the station comprising authentication means for, based upon an authentication algorithm, authenticating a message; and communication means for sending the authenticated message to the host;

the host comprising communication means for receiving an authenticated message; and verification means for verifying the authenticity of the received message by checking the received message with an authentication algorithm corresponding to a station which sent the message;

characterised in that:

the station comprises a memory for electronically storing a plurality of authentication items;

the host comprises a memory for electronically storing the authentication items of the station in association with an identification of the station;

the station comprises constructing means for constructing for each message a corresponding authentication control element; the constructing means being operable to select for the message a part of the plurality of authentication items and to construct the authentication control element from the selected part, where the authentication control element in practical circumstances causes the authentication algorithm to substantially authenticate the corresponding message uniquely; and

the host comprises constructing means for constructing for each received authenticated message an authentication control element from the authentication items associated with a station which sent the message; the construction being the same as performed by the associated station.

2. A system as claimed in claim 1, characterised in that the station comprises a further memory for electronically storing an identification uniquely identifying the station with respect to the host; the authentication means is operative to authenticate the message in dependence on the identification; and the verification means is operative to verify the authenticity of the received message in dependence on an identification of the station which sent the message.

3. A system as claimed in claim 1, characterised in that the authentication items are unique for the station; the station comprises a further memory for electronically storing an identification uniquely identifying the station with respect to the host; the communication means of the station being operative to send the identification to the host in association with an authenticated message; and the host comprises means for locating the authentication items of a station in dependence on an identification received in association with an authenticated message.

4. A system as claimed in claim 1, characterised in that the station comprises modification means for modifying at least one of the authentication items after the authenticating means has authenticated a message and in that the host comprises modification means for modifying at least one of the authentication items for the station in the same way as the station after the verification means has successfully verified an authenticated message received from the station.

5. A system as claimed in claim 4, characterised in that the modification means is operative to modify an authentication item at least partly based on an event independent of the authentication items.

6. A system as claimed in claim 2 or 3, characterised in that the station comprises alteration means for altering the identification associated with the station after the authenticating means has authenticated a message and in that the host comprises alteration means for altering the identification associated with the station in the same way as the station after the verification means has successfully verified a received authenticated message.

7. A system as claimed in claim 1, characterised in that the authentication means comprises data generation means for generating additional data and in that the authentication means is operative to authenticate a message in dependence on the additional data; the additional data in practical circumstances with a high likelihood being different for each message.

8. A system as claimed in claim 7, characterised in that the verification means comprises data generation means for generating additional data for a received authenticated message in a same manner as the identified station and in that the verification means is operative to verify the authenticity of the received authenticated message in dependence on the additional data.

9. A system as claimed in claim 7, characterised in that the authentication means is operative to incorporate the additional data into the message before authenticating the message; and in that the verification means is operative to remove the additional data

from a received authenticated message after having successfully verified the authentication of the message.

10. A system as claimed in claim 1, characterised in that:

the construction means comprises at least one state variable influencing the construction of the authentication control element;

the construction means is operative to update the state variable at least each time a message has been authenticated; and to construct the authentication control element under control of a control vector derived from a selection of the authentication items.

1/2

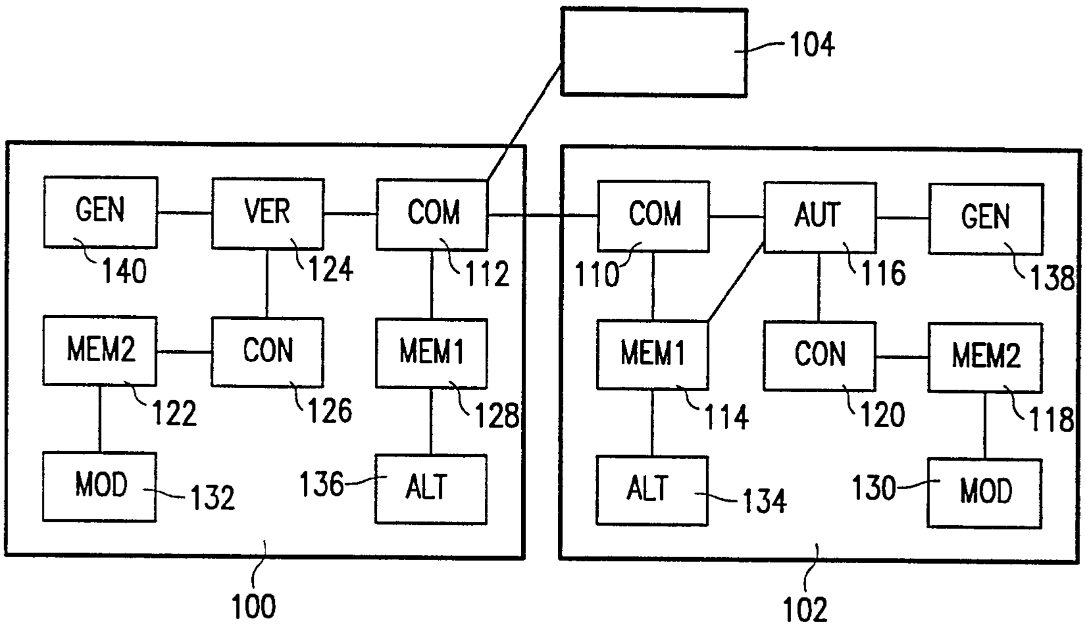

104
GEN
VER
COM
COM
AUT
GEN
140
124
112
110
116
138
MEM2
CON
MEM1
MEM1
CON
MEM2
122
126
128
114
120
118
MOD
132
136
ALT
ALT
134
130
MOD
100
102

FIG. 1

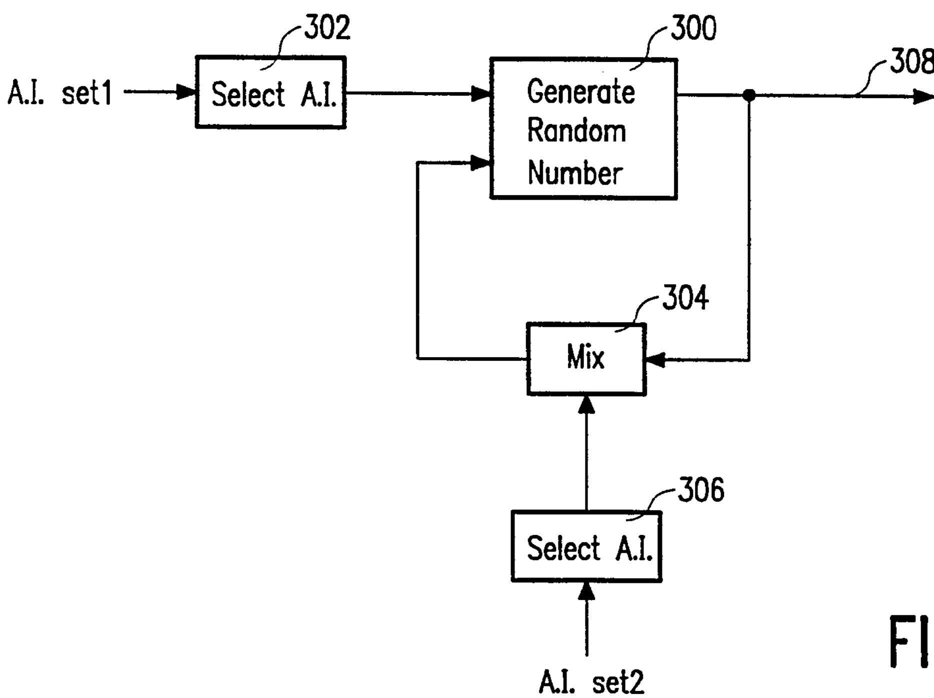
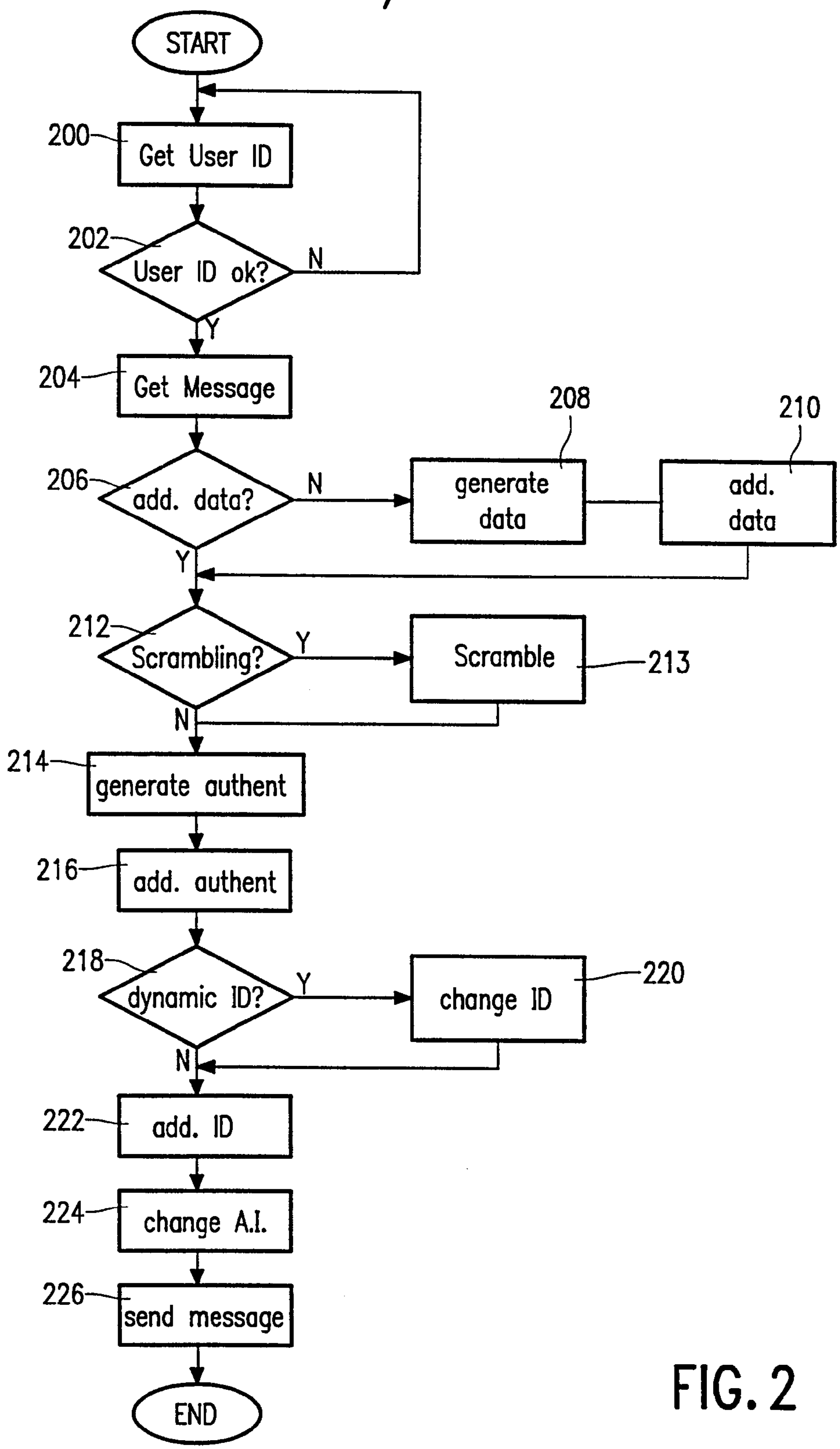

302
300
308
A.I. set1
Select A.I.
Generate Random Number
304
Mix
306
Select A.I.
A.I. set2

FIG. 3



START
200
Get User ID
202
User ID ok?
N
Y
204
Get Message
206
add. data?
N
208
generate data
210
add. data
Y
212
Scrambling?
Y
Scramble
213
N
214
generate authent
216
add. authent
218
dynamic ID?
Y
change ID
220
N
222
add. ID
224
change A.I.
226
send message
END

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 98/00578

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: G06F 12/14, G06F 1/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0737907 A2 (SECURE COMPUTING CORPORATION), 16 October 1996 (16.10.96), column 6, line 44 - column 8, line 8 --	1
A	US 5615277 A (HOFFMAN), 25 March 1997 (25.03.97), column 6, line 52 - column 17, line 3 --	1-10
A	US 4677670 A (HENDERSON, JR.), 30 June 1987 (30.06.87), column 1, line 44 - column 12, line 15; column 3, line 25 - line 39 -- --------	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" erlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 November 1998	06 -11- 1998
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Göran Magnusson Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/IB 98/00578

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0737907 A2	16/10/96	AT 154150 T	15/06/97
		AU 667925 B	18/04/96
		AU 678937 B	12/06/97
		AU 4284793 A	18/11/93
		AU 5081196 A	18/07/96
		CA 2118246 A	28/10/93
		DE 69311331 D,T	30/10/97
		DK 636259 T	07/07/97
		EP 0636259 A,B	01/02/95
		SE 0636259 T3	
		JP 7505970 T	29/06/95
		US 5276735 A	04/01/94
		US 5499297 A	12/03/96
		US 5502766 A	26/03/96
		WO 9321581 A	28/10/93
US 5615277 A	25/03/97	US 5613012 A	18/03/97
		US 5764789 A	09/06/98
		US 5802199 A	01/09/98
		US 5805719 A	08/09/98
US 4677670 A	30/06/87	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 12/56, 29/02 — A3

(11) International Publication Number: WO 98/59470

(43) International Publication Date: 30 December 1998 (30.12.98)

(21) International Application Number: PCT/SE98/01217

(22) International Filing Date: 23 June 1998 (23.06.98)

(30) Priority Data:
9702385-7 23 June 1997 (23.06.97) SE

(71) Applicants *(for all designated States except US)*: TELEFON-AKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE). TELIA AB [SE/SE]; S-123 86 Farsta (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: KANTER, Theo [NL/SE]; Rönninge skolväg 35E, S-144 62 Rönninge (SE). FOGELHOLM, Rabbe [SE/SE]; Turevägen 54 B, S-191 47 Sollentuna (SE).

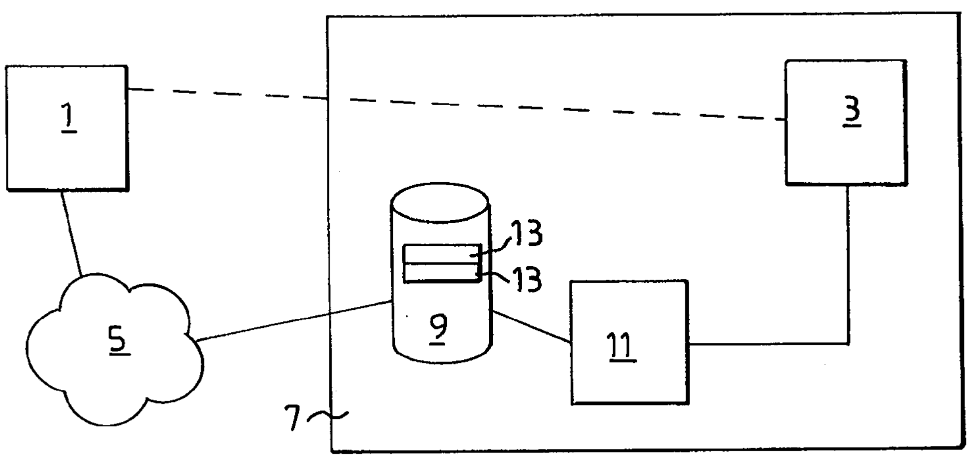
(74) Agents: HERBJØRNSEN, Rut et al.; Albihns Patentbyrå Stockholm AB, P.O. Box 3137, S-103 62 Stockholm (SE).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report: 18 March 1999 (18.03.99)

(54) Title: METHOD AND APPARATUS TO ENABLE A FIRST SUBSCRIBER IN A LARGER NETWORK TO RETRIEVE THE ADDRESS OF A SECOND SUBSCRIBER IN A VIRTUAL PRIVATE NETWORK



(57) Abstract

The present invention relates to an apparatus and a method for use in a virtual private network, VPN, (7, 7'), or a network domain forming part of a larger network, such as the Internet, to enable a first subscriber (1; 1') in the larger network to retrieve the address of a second subscriber (3; 3') in the VPN. The address may be returned to the first subscriber (1; 1') or a connection means (11) may set up the connection between the subscribers (1, 3; 1', 3') automatically.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 98/01217

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 12/56, H04L 29/02
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPIL, EDOC, JAPIO

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	ITU-T Recommendation H. 323, 1996, "Visual telephone systems and equipment for local area networks which provide a non-guaranteed quality of service" Paragraph 6.4, 3.41, 3.43	4-6
Y		1-3,7-12
	--	
Y	IETF RFC 883, Volume, November 1983, P. Mockapetris, "DOMAIN NAMES - IMPLEMEntATION and SPECIFICATION" page 23	1-3,7-12
	--	
A	IETF RFC 1383, Volume, December 1992, C. Huitema, "An Experiment in DNS Based IP Routing", paragraph 2	1-12
	--	

[X] Further documents are listed in the continuation of Box C.   [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 January 1999	22 -01- 1999
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Christina Halldin Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 98/01217

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	IETF RFC 2052, Volume, October 1996, A. Gulbrandsen et al, "A DNS RR for specifying the location of services (DNS SRV)", see the whole document --	1-12
A	EP 0752674 A1 (SUN MICROSYSEMS, INC.), 8 January 1997 (08.01.97), abstract -- --------	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

01/12/98

International application No.
PCT/SE 98/01217

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0752674 A1	08/01/97	JP 9171465 A	30/06/97
		US 5745683 A	28/04/98

Form PCT/ISA/210 (patent family annex) (July 1992)

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 13/00, H04L 9/30 — A1

(11) International Publication Number: WO 99/38081

(43) International Publication Date: 29 July 1999 (29.07.99)

(21) International Application Number: PCT/US99/01583

(22) International Filing Date: 26 January 1999 (26.01.99)

(30) Priority Data:
09/013,122 26 January 1998 (26.01.98) US

(71) Applicant: ASCEND COMMUNICATIONS, INC. [US/US]; One Ascend Plaza, 1701 Harbor Bay Parkway, Alameda, CA 94502 (US).

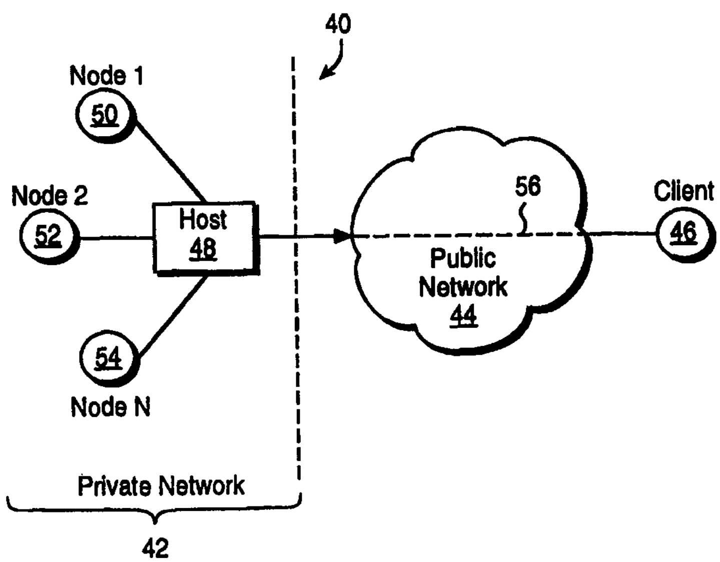
(72) Inventors: PAULSEN, Gaige, B.; 513 Springvale Road, Great Falls, VA 22066 (US). WALKER, Amanda; 2230 Cedar Cove Court, Reston, VA 20191 (US).

(74) Agent: LOHSE, Timothy, W.; Gray Cary Ware & Freidenrich, 400 Hamilton Avenue, Palo Alto, CA 94301 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: VIRTUAL PRIVATE NETWORK SYSTEM AND METHOD



(57) Abstract

A system and method for remote users to access a private network (42) having a first communications protocol via a public network (44), such as any TCP/IP network having a second different communications protocol, in a secure manner so that the remote user appears to be connected directly to the private network (42) and appears to be a node on that private network (42). A host (48) connected to the private network (42) may execute a host software application which establishes and provides a communications path for secure access of the remote client computer (46). An encrypted data stream may be communicated between the host (48) and the client (46) representing traffic and commands on the network.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

VIRTUAL PRIVATE NETWORK SYSTEM AND METHOD

Background of the Invention

This invention relates generally to apparatus and methods for accessing computer networks and in particular to establishing a secure connection between a remote computer and a private computer network using a public computer network.

In the past, organizations and companies have used private (internal) computer data networks to connect its users to each other. These private networks are not accessible to the public and permit sensitive data to be transferred between users within the company. However, due to the increasing numbers of people who need access to the private computer data network and the disparate locations of these people, there are several disadvantages of these conventional private computer networks.

As the number of people in a company grows, the workforce becomes more dispersed among different locations and there are more employees who are mobile, such as salespeople who travel around a region of the United States. For example, some employees may telecommute which requires dial-up access to the private computer data network. The dispersed workforce and the mobile workforce make a private computer data network unmanageable because this mobility requires at least two network connections for each user. In addition, since cellular telephone access has also become more available, additional connections to the network for this access is needed. In addition, full-time telecommuters dramatically increase the number of permanent "remote offices" a company must interconnect which further complicates the private computer data network administration and topology. In addition, as companies increase in size, due to acquisitions, mergers and expansion, the private computer data network must support more remote offices and more network nodes. Thus, as a organization expands, the private computer data network of the organization becomes unwieldy and unmanageable.

Recently, it has become necessary and desirable to permit employees of the company to interact "on-line" with customers and suppliers. This function adds a new dimension of complexity to the private computer data network since multiple private computer data networks must be interfaced together in a delicate balance of integration while maintaining some isolation due to security concerns. The individual networks that are being integrated together typically use different data transfer protocols, different software applications, different data carriers and different network management systems. Thus, interfacing these private computer data networks is a major challenge.

There is also a desire to consolidate and simplify the user interface to the computer network as well as to the software applications being executed by the computer network since it is often difficult to keep on top of each new software application. Thus, the costs of implementing and maintaining a private computer data network is high and is expected to increase in the future as the factors set forth above continue to drive up the costs of the private computer data networks. These high costs are compounded by the high costs for long distance telephone charges for leased lines and switched services. The number of support staff necessary to manage the complex topologies of these private computer data networks also further increases the costs to manage the private computer data networks. In addition, software applications which execute over the private network require separate backup equipment which further complicates the topology and increases the cost of the private computer data network. Thus, the costs and complexity of these private computer data networks are continuing to spiral upwards and there is no foreseeable end in sight.

A typical private computer data network may be used by a organization for some of its communications needs and may carry exclusively data traffic or a mix of voice/video and data traffic. The private computer data network may be constructed with a variety of wide area network (WAN) services that often use the public switched telephone network (PSTN) as a communications medium. A typical network may use high speed leased lines that carry voice, facsimile, video and data traffic between major facilities. These leased lines may include integrated services digital network (ISDN) lines or conventional T1 telephone lines. Because these leased lines are point-to-point connections, a mesh topology is necessary to interconnect multiple facilities. In addition, each leased line must be dedicated to a particular interconnection. A remote office may use switched services over the PSTN, such as ISDN or frame relay. For individual mobile employees, an analog modem may be the best solution for connection to the private computer data network. The private computer data network with all of these different connections, therefore, is very expensive to implement and maintain for the reasons set forth above.

A virtual private network (VPN), on the other hand, may offer the same capabilities as a private computer data network, but at a fraction of the cost. A virtual private network is a private data network that uses a public data network, instead of leased lines, to carry all of the traffic. The most accessible and less expensive public data network currently is the Internet which can be accessed worldwide with a computer and a modem. An Internet-based virtual private network (VPN) is virtual because although the Internet is freely accessible to the public, the Internet appears to the organization to be a dedicated private network. In order to accomplish this, the data traffic for the organization may be encrypted at the sender's end and then decrypted at the receiver's end so that other users of the public network can intercept the data traffic, but cannot read it due to the encryption.

A VPN can replace an existing private data network, supplement a private data network by helping relieve the load on the private data network, handle new software applications without disturbing the existing private data network or permit new locations to be easily added to the network. A typical VPN connects one or more private networks together through the Internet in which the network on each side of the Internet has a gateway and a leased line connecting the network to the Internet. In these typical VPNs, the same protocol for each private network, such as TCP/IP, is used which makes it easier to communicate data between the two networks. To create the VPN, a secure communications path between the two gateways is formed so that the two private networks may communicate with each other. In this configuration, however, each network is aware that the other network is at some other location and is connected via a router. As an example, if a company has a central private network in California and a remote office in Hong Kong, these two private networks may be connected via the VPN which reduces long distance telephone call charges. However, if a single individual is traveling in Hong Kong and want to connect to the private network in California, the individual must incur long distance telephone charges or, if there is a remote office in Hong Kong, then the entire private network must be connected via the VPN to the California private network to communicate data. In addition, with the conventional VPN described, the individual in Hong Kong is aware that he is connected to the Hong Kong network which is in turn connected, via the gateway and the VPN, to the network in California so that the person in Hong Kong cannot, for example, easily use the network resources of the California network, such as a printer.

Thus, a conventional VPN requires the expense of a leased line and a gateway at each end of the VPN and cannot adequately address the needs of a individual who needs access to the private network. In addition, these conventional VPNs cannot easily connect networks which have different networking protocols. In addition, these conventional VPNs cannot be easily used for connecting an individual who needs remote access to the private network since the entire network with a gateway is needed. Thus, the invention provides a virtual private network (VPN) which avoids these and other problems with conventional VPNs and it is to this end that the invention is directed.

Summary of the Invention

In accordance with the invention, a virtual private network system is provided which connects a private data network and a remote client which does not require expensive leased lines or gateways to establish a secure communications path. The system also permits an individual to access the private data network without incurring any long distance telephone charges. In addition, the system permits a private data network and remote client that use one communications protocol to communicate with each other over a public data network that uses a different communications protocol. The system also permits an individual to easily connect to the private date network without a remote private network and the individual appears to be a node on the private network, once connected, so that the individual may access any resources on the private data network.

In accordance with the invention, a system and method for forming a communications path between a public access network and a private access network where the two networks have substantially incompatible transmission protocols is provided. The method comprises establishing a secure communications path over the public access network between a host computer connected to the private network and a remote client computer, encrypting data and commands of the host computer and the client computer, and formatting the encrypted data and commands into a format compatible for transmission over the public access network. The formatted data and commands are then transmitted over the public access network. Once the formatted data and commands has reached its destination, it is decrypted to establish the client computer as a virtual node on the private network. In accordance with another aspect of the invention, a data structure for communicating data for a private data network having a first communications protocol over a public access network having a second communications protocol is provided.

Brief Description of the Drawings

Figure 1 is a block diagram illustrating a conventional virtual private network;

Figure 2 is a block diagram illustrating a virtual private network in accordance with the invention;

Figure 3 is a block diagram illustrating more details of the host computer of Figure 1; and

Figure 4 is a flowchart illustrating a method for establishing a virtual private network and communicating secure data over the virtual private network in accordance with the invention.

Detailed Description of a Preferred Embodiment

The invention is particularly applicable to a system and method for providing a virtual private network which permits remote users to access a private network, such as an AppleTalk network, via a public TCP/IP network, such as the Internet, in a secure manner as if the remote user was one of the nodes on that private network. It is in this context that the invention will be described. It will be appreciated, however, that the system and method in accordance with the invention has greater utility. Before describing the invention, a brief description of a conventional virtual private network (VPN) will be provided.

Figure 1 is a block diagram illustrating a conventional virtual private network (VPN) 20. The VPN includes a first private network 22 and a second private network 24 connected together through a public computer network 26, such as the Internet. The communications protocols for the first and second private networks as well as the public network may be the standard Transmission Control Protocol/Internet Protocol (TCP/IP). Thus, the communications protocols for the private networks are the same as the public network. Each private network 22, 24 includes a gateway 28, 30 which interfaces between the respective private network and the public network. Each gateway encrypts data traffic from the private network which is going to enter the public network and decrypts encrypted data received from the public network. In normal operation, a secure communications path 32, referred to as a tunnel, is formed over the public network that connects the first and second private networks through the respective gateways. The combination of the two private networks and the tunnel over the public network forms the virtual private network (VPN). The VPN is virtual since it is actually using a public network for the connection, but due to the encryption both private networks believe that they have a private network over which data may be sent. For example, a node 34 of the first private network 22 may send data which is encrypted by the gateway 28 through the tunnel 32, and the data is received by the second gateway 30 which decrypts the data and routes it to the appropriate node in the second private network. This conventional VPN, however, does not adequately provide an individual remote user with a system for remotely accessing the private network because the conventional VPN connects two networks with a tunnel and would require the individual to be connected to one of the private networks to utilize the VPN. In addition, this conventional VPN does not connect a remote individual directly to the private network so that a remote user with a VPN connection cannot directly access resources, such as a printer, connected to the private network. This conventional system also does not handle computer networks which have different communications protocols. Now, the virtual private network system in accordance with the invention will be described which overcomes these problems with a conventional VPN.

Figure 2 is a block diagram illustrating a virtual private network (VPN) 40 in accordance with the invention. The VPN may include a private network 42 which communicates data using a first communications protocol, a public network 44 which communicates data using a second communications protocol, and a client node 46 that is connected for secure communications to the private network 42 through the public network 44 as described below. The private network 42 may be any type of computer network, such as an AppleTalk network. The public network may be any type of publicly accessible computer network such as the Internet.

The private network 42 may include a host computer 48, and a plurality of network nodes, such as a first node (NODE_1) 50, a second node (NODE_2) 52, and an nth node (NODE_N) 54 which are all connected to the host computer. In normal operation any node of the private network may share resources with any other node on the network. For example, any node of the private network may share a printer which is attached to the private network. The host computer 48 establishes a secure communications path 56, referred to as a tunnel, through the public network 44 with the remote client 46 by negotiating the communications protocol with the client 46 and authenticating the identity of the client. Once the secure tunnel has been established between the private network 42 through the host computer 48 and the public network 44 with the remote client 46, the remote client is treated as a node of the private network and uses the communications protocol of the private network even though the public network uses a different protocol. Thus, the remote client 46 may access resources connected to the private network, such as a printer, as if the remote client were directly connected to the private network. Therefore, with the VPN in accordance with the invention, the various connections between the remote client and the private network are transparent to the user of the remote client since the user can use the private network in any manner that a user directly connected to the private network can.

With the VPN in accordance with the invention, a gateway at each end of the virtual private network is not required. In addition, data traffic for the private network which has a first data communications protocol may be communicated over a public computer network which has a different communications protocol. In particular, the system encapsulates the data destined for the private data network having a first protocol in a data packet that may be sent over the public network, as described in more detail below. Thus, once the secure virtual private network connection has been established, the remote client may interact with the private network as if the remote client was directly connected to the private network. The virtual private network in accordance with the invention also permits an individual remote user to easily establish a connection with a distant private network without the need for a remote private network and a leased line or long distance telephone charges. Now, more details about the host computer 48 and the remote client 46 in accordance with the invention will be described.

Figure 3 illustrates more details of the host computer 48 and the remote client 46 in accordance with the invention. The host computer 48 may include a central processing unit (CPU) 60, a memory 62 and a host 64 stored in the memory 62. The host may be a software application which is executed by the CPU 60 of the host computer. When a remote client contacts the private network 42 to establish a secure connection, the host 64 may negotiate and establish the secure virtual connection to the remote client 46, as described below. Once the secure connection has been established, the host 64 accepts unencrypted data from the private network, combines the data with a header containing information about the protocol of the private data network, encrypts the data and the header, and communicates the encrypted data and header, over the secure communications path, to the remote client. The host also receives encrypted data with a header from the remote client, decrypts the data and the header, and passes the data traffic onto the appropriate node in the private network based on the header information, as described below.

Similarly, at the remote client 46, a client software application 66 stored in a memory 68 in the client computer 46 is executed by a central processing unit (CPU) 70 in the client computer 46. The client 66 negotiates and establishes the secure communications path with the host computer, combines the data with an appropriate header, encrypt the data traffic and the header destined for the client computer, and communicate the encrypted data to the host computer. The client also receives encrypted data traffic from the host computer, decrypts it, and passes the data traffic onto other software application which are being executed by the CPU 70. Thus, the virtual private network in accordance with the invention is software application based so that expensive hardware, such as a gateway and leased lines, are not necessary. The software applications also permit the data between the client and host, which have a first communications protocol, to be communicated over a public computer network which has a second different communications protocol. Now, a method for establishing and communicating data traffic over the virtual private network in accordance with the invention will be described.

Figure 4 is a flowchart illustrating a method 100 for establishing and communicating data over the virtual private network in accordance with the invention. An example of the phases and data formats for the communications between an AppleTalk network host and an AppleTalk remote client over the Internet will be described below, but the invention is not limited to that example and may be used to communicate data between any hosts and remote clients having a different communications protocol than the public data network. To begin the method, the remote client may request a connection to the host by any conventional method.

In step 102, once the initial unsecure connection has been established between the host and the client, a protocol negotiation phase occurs in which the host and the client negotiate the parameters that will govern the subsequent communications between the host and the client. The negotiated parameters may include the protocol version, the compression level, and the encryption technique. Each of these parameters has a default setting that must be available for either the host or the remote client to request so that there is a minimum set of functionality which may be implemented. To ensure backwards compatibility of any host or remote client, each host or client will implement at least a first protocol version so that there is backwards compatibility for future versions. These parameters will be described in more detail below. In addition, for the encryption parameter, each host and remote client must be able to support both data encryption standard (DES) type encryption as well as some form of non-DES encryption to permit communications between hosts and clients that are licensed for use within the United States as well as outside of the United States. The invention may use a plurality of different well-known non-DES encryption methods and these encryption methods will not be described here. The protocol negotiation phase is started when the connection is established and is initiated by the remote client sending the host a Protocol Request in which it communicates which protocol version it would like to use and any options, such as the encryption, that it would like to use. The host then sends the remote client a Protocol Response verifying the protocol version number and any options. An example of the data formats of the Protocol Request and Protocol Response in the context of an AppleTalk network are provided below.

Once the protocol has been negotiated, it is determined, in step 103, if an optional session key negotiation phase 104 is going to occur. In the first protocol version, the session key negotiation phase is optional, but later versions of the protocol will require the session key negotiation phase. The session key negotiation phase is thus entered if a session key bit in the Protocol Request is set during the protocol negotiation phase. During the session key negotiation phase, data is exchanged between the host and remote client for the purpose of setting up an encryption key that is used for the remainder of the communication. In a preferred embodiment, a well known Diffie-Hellman key exchange method is used, but any other conventional key exchange method may be used. If the session key phase and the Diffie-Hellman key exchange method are not being used, the encryption key is chosen during an authentication phase 106, as described below. The data communicated during the session key negotiation phase may include a length word indicating the length of the data and the data. The data flow is bi-directional and is completed when the host and the remote client have agreed on a session key. If the system determines, in step 105, that a session key has been established, an authentication phase 106 is entered. In the event that a session key is not successfully negotiated during the session key negotiation phase, the method proceeds to a teardown phase 110 in which the communications between the host and the remote client is terminated and the methods ends.

During the authentication phase 106, the remote client and the host negotiate what type of authentication is used for the communications and then provides challenges and responses to authenticate the identity of the remote client. Due to the wide variety of security requirements and methods, the host must, at a minimum, send a request with at least one default authentication type identifier and an associated challenge. However, if the host has the ability to use more than one authentication method, then the host may send the remote client, in a Authentication Request, more than one authentication type identifier and their associated challenges as described below. Thus, to start the authentication phase, the host may communicate an authentication request, as described below, to the remote client. The authentication request may include one or more authentication type/authentication challenge data pairs. In response to the authentication request, the remote client communicates an authentication response back to the host which includes exactly one authentication type/response data pair. If the host sends more than one authentication type/challenge pair, the remote client selects a particular authentication type and responds with the authentication type/response pair for only that particular authentication type. An example of the types of authentication methods is set forth below.

If the session key negotiation phase is not used, then, during a successful authentication phase, an implicit session key may be generated by the remote client. In a preferred embodiment, the session key may be generated by the following steps.

First, a Unicode string containing the password from the client is concatenated with the challenge from the authentication request. Next, a SHA-1 hash value over the resultant concatenated data is calculated and the initial bytes of the hash value may then be used as the session key which may be communicated back to the host.

In response to the authentication response, the host determines if the response was successful or not in step 107. If the response was successful (i.e., an appropriate response to the challenge was received which verifies the identity of the remote client), a success data structure is sent to the remote client and the method goes to an established phase 108, as described below. If the response was not successful (i.e., an appropriate response to the challenge was not received so that the identity of the remote client can not be verified), then an error code is sent to the remote client and the teardown phase 110 is entered.

During a typical successful secure communications session, most of the time is spent in the established phase 108 in which encrypted data including the header is communicated between the remote client and the host. The header, as described below, contains information required by the communications protocol of the private network (i.e., the host and the remote client) to appropriately route data. Thus, the communications protocol information for the private network is embedded in the encrypted data packet so that the data destined for the private data network may be communicated over the public network having a different communications protocol. For each piece of encrypted data sent during the established phase, the data may be preceded by a length and flag word which contains the length of the data in bytes and six bits of flags. Since the data is typically sent over a TCP/IP based public network, a PUSH bit in the flag bits must be set to accelerate the processing of the transactions once a complete unit of data has been received.

If an unsuccessful session key negotiation, an unsuccessful authentication, or the end of the established phase occurs, then the tear down phase 110 is begun. During the tear down phase, there is no data traffic between the remote client and the host and the communications channel is forcibly closed by either the remote client or the host. During the teardown phase, when one side shuts down the communications channel , an acknowledgment from the other side may consist of shutting down the connection from that side as well so nothing remains of the communications path. After the teardown phase, the method has been completed. The method, therefore sets up a communication session as needed and then tears down the communications path once the communications have been completed.

Now, an example of the data formats for a system and method in accordance with the invention for communicating AppleTalk data between a remote client and a host over a TCP/IP public network, such as the Internet, will be described. As described above, the virtual private network in accordance with the invention may connect any private network having a first communications protocol to a public network having a second different communications protocol securely to permit remote users to access the private network in a secure manner wherein the remote user appears to be one of the nodes in the private network. In this example, the data formats for each of the communications phases are set forth and explained. For each different private data network with a different communications protocol, these data formats will vary slightly. The bytes of these data formats are sent across the network connection path over the Internet using a Network Byte Order protocol in which the most significant byte is communicated first.

To better understand the utility of the invention in the context of a connection between an AppleTalk private network and a AppleTalk remote client over the TCP/IP-based Internet, the differences between the protocol for the AppleTalk network and the Internet will be described before describing the data formats for this example. AppleTalk is a proprietary suite of networking protocols which is designed for plug-and-play operation whereas TCP/IP is designed to be administered. In particular, the Internet or any other TCP/IP network has been designed such that each node on the Internet is permanently assigned a unique IP address by a quasi-governmental entity. AppleTalk, on the other hand, assigns a node or device number to a node or device when the nodes or devices are actually placed on the network to provide the plug-and-play functionality. Therefore, the two networking protocols assigns network numbers in different manners.

AppleTalk also has a smaller network number range than the Internet and is not centrally administered so that AppleTalk networks can not be arbitrarily connected to each other without substantial planning to ensure that the connected nodes do not have overlapping network numbers. In AppleTalk, there is also a service location protocol that permits users to locate servers and network devices, such as printers, and AppleTalk has the concept of a "zone" which provide a level of scoping for the service location protocol. In order to access the network services on a particular network, you must have access to the particular zone. One advantage of the invention is that the remote client can avoid the network number and zone addressing by connecting the user of the remote client directly on the AppleTalk network as a virtual node in the zone of the host computer in a secure manner. Thus, once the user of the remote client is securely connected to the AppleTalk network over the Internet, the user sees all of the devices of the AppleTalk network, such as printers and file servers, in a familiar manner which permits them to access any device on the private network. Now, an example of the data formats for the invention when connecting an AppleTalk private network and a remote client over the Internet will be described.

During the protocol negotiation phase, as described above, there is a protocol request from the host and a protocol response from the remote client. The data formats of the protocol request and protocol response are set forth in Tables 1 - 3 below.

Table 1- Protocol Request

Byte Offset	Width	Contents
0	2 bytes	Total Bytes: Total number of bytes in the transaction (excluding this field)
2	2 bytes	Protocol Version: Protocol version requested
4	2 bytes	Options Bytes: Length of the following data bytes
6	specified by the previous field	Options: Any options to be requested

In version 1 of the protocol, the Total Bytes in the protocol request is 6, the Protocol Version is 1, the Options Bytes is 2, and the Options field will contain two bytes which represent 16 individual flag bits. For other versions of the protocol, these fields may contain different values. The meanings of the flag bits in the protocol request data format are set forth below in Table 2.

Table 2 - Option Flag Bits Format

Byte Location	Meaning
15-2	Reserved for future options. These must be 0 in the first version of the protocol.
1	Use session key negotiation. If this bit is set, the requester wants to use the Session Key Negotiation phase. If not, it is requested that the phase be omitted.
0	Use DES encryption. If this bit is set, the requester wants to use DES encryption. If it is not set, an alternate encryption method is to be used.

Thus, using the options fields in the first version of the protocol, the session key negotiation phase and the type of encryption may be chosen. With future versions of the protocol, additional options may be selected. The format of the Protocol Response will now be described with reference to Table 3.

Table 3 - Protocol Response

Byte Offset	Width	Contents
0	2 bytes	Total Bytes: Total number of bytes in the transaction (excluding this field)
2	2 bytes	Protocol Version: Protocol version to be used
4	2 bytes	Options Bytes: Length of the following data bytes
6	specified in Options Bytes	Options: Any options that are in use

The protocol response data uses a similar data format to the Protocol request, and contains the same data. However, when returned from the Host to the Client in the Protocol Negotiation phase, this data establishes the actual communication protocol and data format to be followed during the Established phase. The data communicated during the protocol negotiation phase is unencrypted since the secure communications path has not yet been established. Now, the data formats for the optional session key negotiation phase will be described.

The session key negotiation phase, as described above, may include the session negotiation request and the session negotiation response. The data format for both of these pieces of data are identical for all responses and requests. In particular, each data packet contains a 2 byte length field followed by the data used for the negotiation of the session key for use in the well-known Diffie-Hellman key exchange method. Once again, the data is sent unencrypted since no secure communications channel has been established.

The authentication phase, as described above, may include an authentication request and an authentication response, whose data formats are set forth below in Tables 4-6.

Table 4 - Authentication Request

Byte Offset	Width	Contents
0	2 bytes	Total Bytes: Total number of bytes in the transaction (excluding this field)
2	2 bytes	Authentication Type: Identifies the authentication type
4	2 bytes	Challenge Bytes: The number of bytes that follow for the challenge (0 or more)
6	specified in Challenge Bytes	Challenge: The data for the challenge in the authentication. The exact contents vary based on the authentication method.

As described above, this data must contain at least one authentication type/challenge pair, but may contain more than one authentication type/challenge pair if the host supports more than one type of authentication. In version 1 of the protocol, the Authentication Type must be one of types set forth in Table 5.

Table 5 - Authentication Types

Authentication Type	Description
0	No authentication. No bytes follow for the challenge (may not be supported by any server). A 0-length response is expected by Hosts which request this method.
1 - Clear Text authentication.	There is no challenge (may not be supported by any server). A 0-length challenge is sent, and the Host expects the user name and password of the client to be sent in clear text.
2	Challenge-Handshake Authentication Protocol (CHAP) - There is an 8-byte encrypted challenge. A 24-byte response is expected by the Host. This method MAY be supported by Hosts and Clients.
3	NT RAS compatible CHAP - There is an 8-byte encrypted challenge. A 16-byte response is expected by the Host. This method MUST be supported by all Hosts and Clients.

As shown, there are several different authentication methods which may be used. The default authentication method is the NT RAS compatible CHAP with an 8 byte challenge and a 16 byte response. Again, since no secure communications path has been established, this data is sent unencrypted. Now, the data format of the authentication response is described with reference to Table 6.

Table 6 - Authentication Response

Byte Offset	Width	Contents
0	2 bytes	Total Bytes: Total number of bytes in the transaction (excluding this field)
2	2 bytes	Authentication Type: Identifies the authentication type
4	2 bytes	Response Bytes: Number of bytes in the authentication response
6	specified in Response Bytes	Response: The data which responds to the Challenge. The length and exact contents vary based on the authentication type and the challenge.
Response Bytes +6	up to 32	User Name: The clear text version of the user name. The name is terminated by the end of the data (based on Total Bytes).

This authentication response data must contain exactly one response to one of the Authentication Type/Challenge pairs in the preceding Authentication Request. The Client may choose which of the pairs to respond to if more than one appears in the Authentication Request. The User Name in the response specifies which user is requesting access and is used in conjunction with the Response to authenticate the user. This data is also sent unencrypted, unless a session key has been negotiated previously in the Session Key Negotiation phase, in which case it is encrypted.

During the initial portion of the established phase, there may be a success data structure or a failure data structure and then during the actual established phase there may be a data structure for data communicated to the remote client and a data structure for data communicated to the host. These data structures are set forth below in Tables 7 - 11. If a successful secure connection is established, then a connections success data structure, as set forth in Table 7 is sent to the remote client.

Table 7 - Connection Success

Byte Offset	Width	Contents
0	2 bytes	Total Bytes: Total number of bytes in the transaction (excluding this field)
2	2 bytes	Success: always contains 0
4	2 bytes	Client Network Number: the assigned network number for the Client
6	1 byte	Client Node Number: the node number of the Client for the nearest AppleTalk Bridge
7	1 byte	Bridge Node Number: the node number of the nearest AppleTalk Bridge
8	2 bytes	Bridge Network Number: the network number of the nearest AppleTalk Bridge
10	2 bytes	Network Range Start: The start of the network range for the AppleTalk network connected to the Host
12	2 bytes	Network Range End: The end of the network range for the AppleTalk network connected to the Host

This successful connection data is sent by the Host when a connection is successfully established between the Client and the Host. It contains the data necessary to configure the AppleTalk connection on the Client side. The connection success data structure thus contains the embedded information about the private data network communications protocol so that private network data may be communicated over the public network which has a different communications protocol. For example, the Bridge Node Number and Bridge Network Number specify AppleTalk specific network information, such as the AppleTalk default Bridge (or Router) on the network that the Host resides on. This embedded private data network information permits the client and the host to format their data formats, as set forth in Tables 10 and 11, for the particular connection to the particular type of private data network. This embedded information also permits the remote client to be treated as a virtual node of the AppleTalk network so that any devices, such as printers or file servers, on the private network may be accessed by the user of the remote client. The connection success data structure is sent unencrypted, unless a session key has been negotiated in the Session Key Negotiation phase, in which case it is encrypted. The connection failure data format is set forth in Table 8.

Table 8 - Connection Failure

Byte Offset	Width	Contents
0	2 bytes	Total Bytes: Total number of bytes in the transaction (excluding this field)
2	2 bytes	Error Code: Contains the error code sent by the Host

This connection failure data is sent by the Host when a connection cannot be successfully established between the Client and the Host. It contains a length field and only one other field, an Error Code field. The error code field contains an optional representation of why the connection failed. As a default, the host may always return an "Undefined Error" message, which gives no information on why it rejected the request. An example of the error codes are set forth below in Table 9.

Table 9 - Error Codes

Error Code	Description
1	Unsupported Authentication. This is returned when the Client sent an Authentication Response for an Authentication type which was not in the Authentication Request.
2	Failed Authentication. The specified User Name and Response were not valid for the authentication type and Challenge specified. Note: This could be any kind of error from unknown user to invalid password.
3	No Free Ports. The Host does not have any available ports.
4	Already Logged On. The specified User Name is already in use on this server, and multiple logins of the same user are disallowed.
OxFFFF	Undefined Error. An error prevented the connection from succeeding.

This error data is sent unencrypted, unless a session key has been negotiated in the Session Key Negotiation phase, in which case it is encrypted. If the connection failure data structure is sent, then the communications session ends. If a successful connection is established, then data is communicated between the host and the client using the data format for established data to the remote client as set forth in Table 10.

Table 10 - Established Data (To Client)

Byte Offset	Width	Contents
0	2 bytes	Length and Flags: contains the length of the following data in the low 10 bits and a set of reserved flags in the upper 6 bits.
2	2 bytes	Source Network: the network number that sent the packet.
4	1 byte	Source Node: the node number that sent the packet.
5	1 byte	Destination Socket: the socket that the packet is being sent to.
6	1 byte	Source Socket: the socket that sent the pocket.
7	1 byte	Type: the AppleTalk type of the packet.
8	Specified by the Length	Payload: the data from the original packet.

This data is sent from the Host to the Client during the established phase. As shown, the data contains the AppleTalk specific information to route the data packet to the client. This data is always encrypted. The basic format (with no flags set) contains data from one packet on the AppleTalk network that is destined for the Client. An example of the data format for data from the remote client to the host is set forth in Table 11.

Table 11 - Established Data (From Client)

Byte Offset	Width	Contents
0	2 bytes	Length and Flags: contains the length of the following data in the low 10 bits and a set of reserved flags in the upper 6 bits.
2	2 bytes	Destination Network: the network number the packet is being sent to.
4	1 byte	Destination Node: the node number the packet is being sent to.
5	1 byte	Destination Socket: the socket that the packet is being sent to.
6	1 byte	Source Socket: the socket that sent the packet.
7	1 byte	Type: the AppleTalk type of the packet.
8	Specified by the Length	Payload: the data for the packet.

This data is sent from the remote client to the host during the established phase in order to communicate data packets. The data includes AppleTalk specific information to route the client's data packets to the appropriate node on the private data network. The established data from the remote client to the host is always encrypted to ensure a secure communications channel. The basic format (without any flags set) contains data from one data packet that the remote client is sending to the host which is the AppleTalk network. There are not any special data formats for the teardown phase since no data is communicated between the remote client and the host during the teardown phase.

In summary, the invention provides a virtual private network system between a private data network and a remote client which does not require expensive leased lines or gateways to establish a secure communications path in which the remote client becomes a virtual node of the private network. The system also permits an individual to access the private data network without incurring any long distance telephone charges. In addition, the system permits a private data network and remote client that use a first communications protocol to communicate with each other over a public data network that uses a different communications protocol. The system also permits an individual to easily connect to the private date network as a virtual node without a remote private network and the individual appears to be a node on the private network, once connected, so that the individual may access any resources on the private data network.

In operation, a user of the remote client establishes a secure connection with the host of the private computer network through the authentication process so that the remote client is a virtual node of the private network. The user may then transmit data and commands in the private network's communication protocol over the public network through the secure communications path and receive data and commands back from the private network. For example, the user of the remote client may issue a print command to a printer attached to the private network, that print command is encapsulated in an encrypted data packet sent over the public access network, the host computer decrypts the print command and passes the print command on to the printer attached to the private network. Thus, the remote client is a virtual node of the private network and the user of the remote client may access any of the resources of the private network as if the remote client was an actual physical node of the private network.

While the foregoing has been with reference to a particular embodiment of the invention, it will be appreciated by those skilled in the art that changes in this embodiment may be made without departing from the principles and spirit of the invention, the scope of which is defined by the appended claims.

Claims:

1. A method for forming a virtual node for a private access network having a private access communications protocol over a public access network having a public access communications protocol, the virtual node being a remote client computer and the method comprising:

establishing a secure communications path over the public access network between a host computer connected to the private network and a remote client computer to establish the remote client computer as a virtual node of the private network;

generating a data packet to be transmitted over the secure communications path, the data packet including data and information about routing the data in the data packet in accordance with the private access communications protocol;

encrypting said data packet;

encapsulating said encrypted data packet into second data packet having a format compatible with the public access communications protocol;

transmitting the second data packet over the public access network;

unpacking the encrypted data packet from said second data packet; and

decrypting the data packet received from the public access network to route the data in the data packet over the private access network using the information about the private access communications protocol.

2. The method of Claim 1, wherein said establishing further comprises negotiating a communications protocol compatible with the private network between the host computer connected to the public access network and the remote client computer, and authenticating the identity of the remote client computer.

3. The method of Claim 2, wherein the authentication comprises generating a challenge at the host computer, communicating said challenge to the remote client computer, and receiving a challenge response from the remote client computer.

4. The method of claim 1 further comprising negotiating a session key for communicating between the host and the client.

5. The method of Claim 1, wherein generating the information in the data packet comprises generating a network node identification number for the remote client node.

6. The method of Claim 5, wherein said private access network comprises an AppleTalk communications network.

7. The method of Claim 6, wherein said public access network comprises the Internet.

8. A virtual node for a private access network having a private access communications protocol over a public access network having a public access communications protocol, the virtual node being a remote client computer and comprising:

means for establishing a secure communications path over the public access network between a host computer connected to the private network and a remote client computer to establish the remote client computer as a virtual node of the private network;

means for generating a data packet to be transmitted over the secure communications path, the data packet including data and information about routing the data in the data packet in accordance with the private access communications protocol;

means for encrypting said data packet;

means for encapsulating said encrypted data packet into second data packet having a format compatible with the public access communications protocol;

means for transmitting the second data packet over the public access network;

means for unpacking the encrypted data packet from said second data packet; and

means for decrypting the data packet received from the public access network to route the data in the data packet over the private access network using the information about the private access communications protocol.

9. The virtual node of Claim 8, wherein said establishing means further comprises means for negotiating a communications protocol compatible with the private network between the host computer connected to the public access network and the remote client computer, and means for authenticating the identity of the remote client computer.

10. The virtual node of Claim 9, wherein the authentication means comprises means for generating a challenge at the host computer, means for communicating said challenge to the remote client computer, and means for receiving a challenge response from the remote client computer.

11. The virtual node of claim 8 further comprising negotiating a session key for communicating between the host and the client.

12. The virtual node of Claim 8, wherein said means for generating the information in the data packet comprises means for generating a network node identification number for the remote client node.

13. The virtual node of Claim 12, wherein said private access network comprises an AppleTalk communications network.

14. The virtual node of Claim 13, wherein said public access network comprises the Internet.

FIG. 1 (Prior Art)

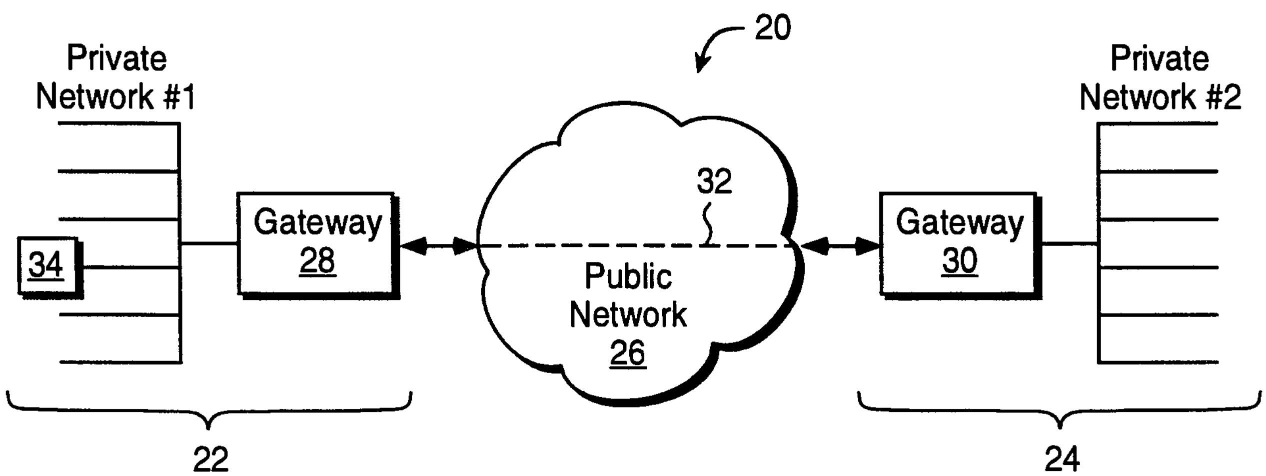


FIG. 2

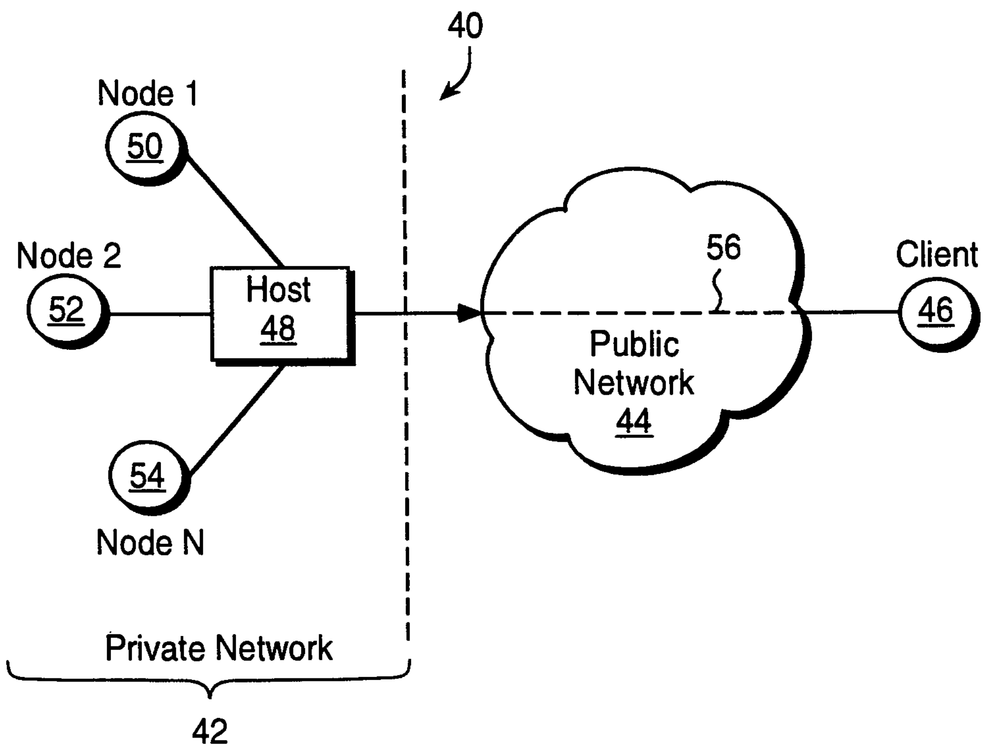


FIG. 3

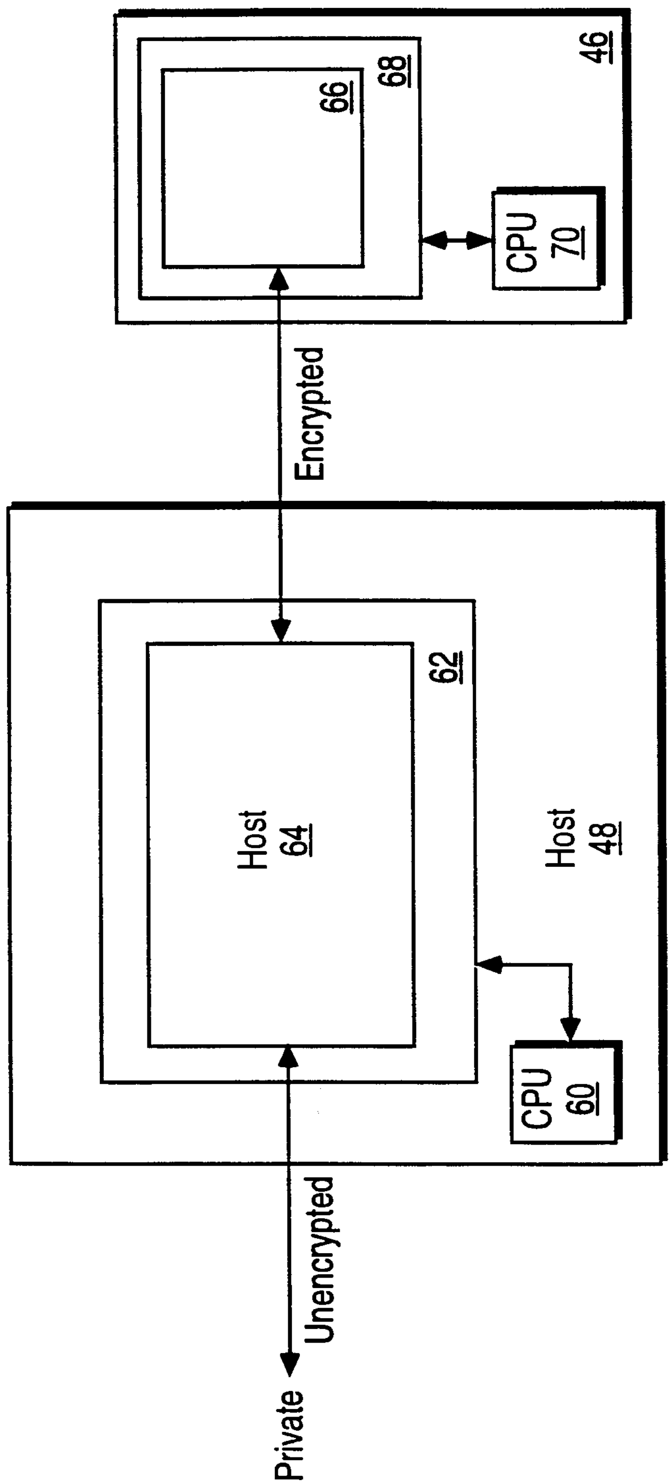
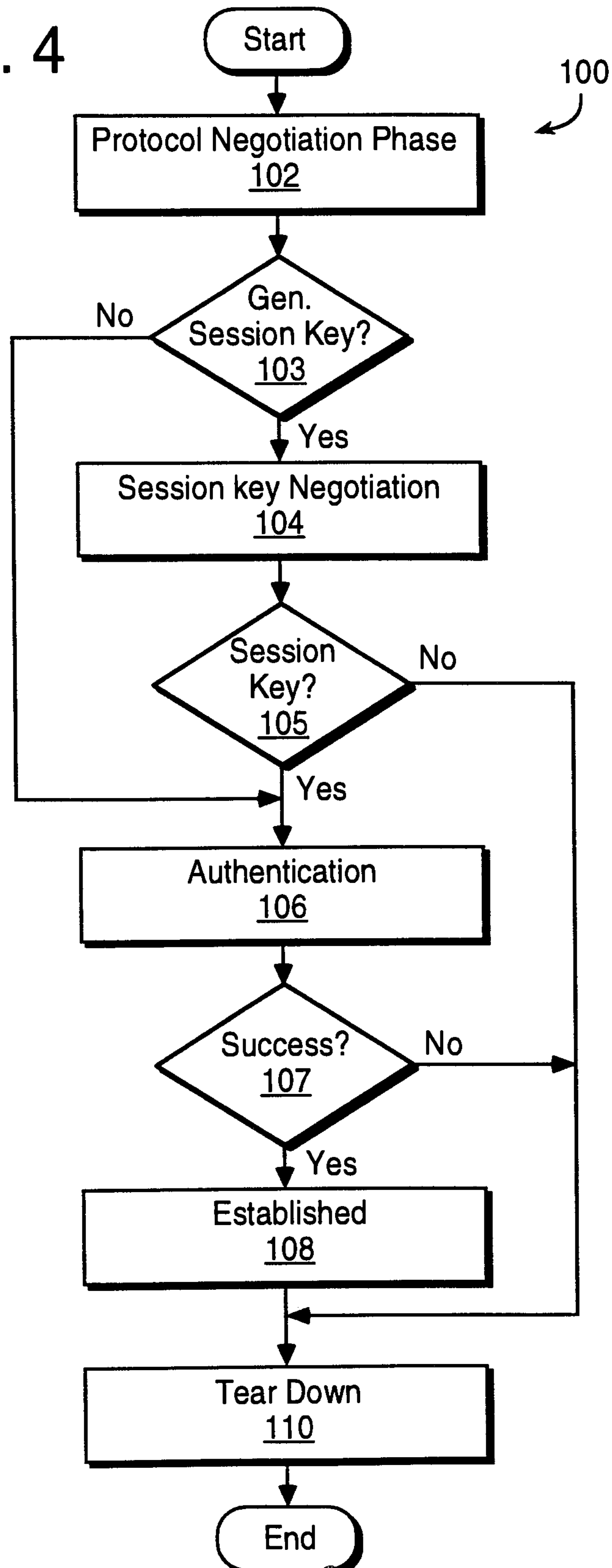

66
68
46
CPU
70
Encrypted
62
Host
64
Host
48
CPU
60
Unencrypted
Private

FIG. 4


Start
100
Protocol Negotiation Phase
102
Gen. Session Key?
103
No
Yes
Session key Negotiation
104
Session Key?
105
No
Yes
Authentication
106
Success?
107
No
Yes
Established
108
Tear Down
110
End

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/01583

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 13/00; H04L 9/30
US CL : 709/245 , 229 ; 380/30
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/245 , 229, 228, 226; 380/30 , 23

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, Internet
Search terms : private and public network, protocols, authentication, session key, encrypt, decrypt, encapsulation.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,416,842 A (AZIZ) 16 MAY 1995, Abstract, Figs. 2 and 5 and 6, col. 4 line 65 - col. 5 line 48, col. 6 lines 3-35 and lines 40-51, col. 7 lines 16-35, col. 7 line 63 - col. 8 line 2	1-14
Y	US 5,550,984 A (GELB) 27 AUGUST 1996, Abstract, Fig. 1, col. 5 line 45 - col. 6 line 51, col. 7 line 58 - col. 8 line 19	1-14
Y	US 5,548,646 A (AZIZ ET. AL.) 20 AUGUST 1996, Abstract, Figs. 5 and 6, col. 9 lines 1-50, col. 10 line 32 - col. 11 line 67	1-14
Y,P	US 5,835,726 A (SHWED ET. AL.) 10 November 1998, Abstract, Fig. 21, col. 20 line 41 - col. 21 line 7, col. 22 line 19 - col. 23 line 9.	1-14

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 MAY 1999	02 JUN 1999

Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	AHMAD MATAR
Facsimile No. (703) 305-3230	Telephone No. (703) 305-4731

Form PCT/ISA/210 (second sheet)(July 1992) ★

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q

A2

(11) International Publication Number: WO 99/48303

(43) International Publication Date: 23 September 1999 (23.09.99)

(21) International Application Number: PCT/US99/05900

(22) International Filing Date: 18 March 1999 (18.03.99)

(30) Priority Data:
09/040,898 18 March 1998 (18.03.98) US

(71) Applicant: CISCO TECHNOLOGY, INC. [US/US]; 170 West Tasman Drive, San Jose, CA 95134 (US).

(72) Inventors: COX, Dennis; 6800 McNeil Drive #828, Austin, TX 78729 (US). MCCLANAHAN, Kip; 3112 Kerbey Lane, Austin, TX 78703 (US).

(74) Agent: SHOWALTER, Barton, E.; Baker & Botts, L.L.P., 2001 Ross Avenue, Dallas, TX 75201-2980 (US).

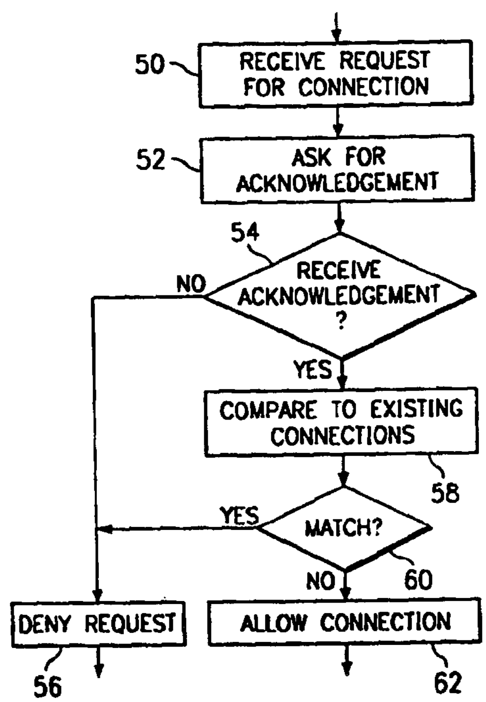
(81) Designated States: AE, AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD FOR BLOCKING DENIAL OF SERVICE AND ADDRESS SPOOFING ATTACKS ON A PRIVATE NETWORK

(57) Abstract

A method is provided for blocking attacks on a private network (12). The method is implemented by a routing device (10) interconnecting the private network (12) to a public network (14). The method includes analyzing an incoming data packet from the public network (14). The incoming data packet is then matched against known patterns where the known patterns are associated with known forms of attack on the private network (12). A source of the data packet is then identified as malicious or non-malicious based upon the matching. In one embodiment, one of the known forms of attack is a denial of service attack and an associated known pattern in unacknowledged data packets. In another embodiment, one of the known forms of attack is an address spoofing attack and an associated known pattern is a data packet having a source address matching an internal address of the private network (12).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

METHOD FOR BLOCKING DENIAL OF SERVICE AND ADDRESS SPOOFING ATTACKS ON A PRIVATE NETWORK

TECHNICAL FIELD OF THE INVENTION

This invention relates in general to communication systems, and more particularly to a method for blocking denial of service and address spoofing attacks on a private network.

BACKGROUND OF THE INVENTION

Corporate and other private networks often provide external access outward and inward through Internet gateways, firewalls or other routing devices. It is important for these routing devices to defend the private network against attackers from the outside as well as to allow access to the private network by authorized users. However there are numerous forms of attack on conventional routing device that can incapacitate the devices and interfere with an associated private network. The problem of keeping unauthorized persons from accessing data is a large problem for corporate and other information service management. Routing devices, such as gateways, firewalls and network routers lack important safeguards to block or prevent attacks. In particular, the number of denial service attacks have risen dramatically in recent years. Further, IP spoofing incidents occur with increasing frequency.

A denial of service attack consists of repeatedly sending requests for connections to different hosts through and/or behind the routing device. Typically, the host will wait for acknowledgment from the requester.

Because a host can only handle a finite number of requests (for example, 1 to n, where n depends on the resources available to the host), the attacker can crash or "flood" a host with requests to the point of disrupting network service (host/server/port) to users.

Another form of attack is address spoofing which can be used by unauthorized third parties to gain access to a private network. This attack involves the attacker identifying a valid internal network address within the private network. The attacker then requests access to the private network through the routing device by spoofing that internal network address. Conventional routing devices typically are not sophisticated enough to determine that such a request should be denied (i.e., because an external request can not originate from an internal address) and will allow access to the attacker. Address spoofing attacks can be carried out against various types of networks and network protocols such as IPX/SPX, MAC layer, Netbios, and IP.

It is therefore advantageous to provide facilities within a routing device that block denial of service, address spoofing and other attacks on an associated private network.

SUMMARY OF THE INVENTION

In accordance with the present invention, a method for blocking denial of service and address spoofing attacks on a private network is disclosed that provides significant advantages over conventional network routing devices.

According to one aspect of the present invention, the method is implemented by a routing device interconnecting the private network to a public network. The method includes analyzing an incoming data packet from the public network. The incoming data packet is then matched against known patterns where the known patterns are associated with known forms of attack on the private network. A source of the data packet is then identified as malicious or non-malicious based upon the matching. In one embodiment, one of the known forms of attack is a denial of service attack and an associated known pattern is unacknowledged data packets. In another embodiment, one of the known forms of attack is an address spoofing attack and an associated known pattern is a data packet having a source address matching an internal address of the private network.

A technical advantage of the present invention is the enabling of a routing device to the identify a denial of service attack and to block such an attack from tying up the routing device.

Another technical advantage of the present invention is enabling a routing device to identify an address spoofing attack and to block such an attack.

A further technical advantage of the present invention is an ability for the routing device to track information about the attacker to allow preventive measures to be taken.

Other technical advantages should be readily apparent to one skilled in the art from the following figures, description, and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the present invention and advantages thereof may be acquired by referring to the following description taken in conjunction with the accompanying drawings, in which like reference numbers indicate like features, and wherein:

FIGURE 1 is a block diagram of an communication system including a routing device and an associated private network;

FIGURE 2 is a flow chart of one embodiment of a method for blocking attacks on a private network according to the present invention;

FIGURE 3 is a flow chart of one embodiment of a method for blocking an address spoofing attack according to the present invention; and

FIGURE 4 is a flow chart of one embodiment of a method for blocking a denial of service attack according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

FIGURE 1 is a block diagram of an communication system including a routing device 10 and an associated private network 12. Routing device 10 provides a connection between corporate private network 12 and an Internet cloud 14. Routing device 10 can include a gateway, firewall or other device interconnecting private network 12 and Internet cloud 14. In operation, routing device 10 allows internal users within private network 12 to gain access to Internet cloud 14. Routing device 10 also allows external users connected to Internet cloud 14 to gain access to private network 12. A significant and growing problem is that an attacker 16 may try to gain access to or disrupt private network 12 through Internet cloud 14.

Denial of service and address spoofing are two common forms of attack that might be used by attacker 16. In general, a denial service attack is one in which attacker 16 attempts to prevent others from using private network 12. A denial service attack works if routing device 10 spends all of its time processing requests and cannot respond quickly enough to satisfy additional requests. An Address spoofing attack is on in which attacker 16 fakes an internal address to get around or into standard address filtering schemes. According to the present invention, routing device 10 is enabled with a method for blocking these and other types of attacks by analyzing incoming data packets.

Thus, one possible occurrence is that attacker 16 will try to get into private network 12 by spoofing an address that exists inside private network 12. This is intended to allow attacker 16 to gain access and impersonate an internal user. When a packet from attacker 16 reaches routing device 12, an attack blocking component, according to the present invention, will notice that the address matches one that exists within private network 12. Because incoming packets should not be the same as outgoing packets, the attack blocking component can deny access to private network 12 and record the information about the attack for use by the system administrator. Attacker 16 can also try to deny access to all external users by conducting a denial of service attack. This involves attacker 16 flooding private network 12 or routing device 10 by sending an extremely large number of packets. For example, attacker 16 may send 30,000 or more packets. According to the present invention, the attack blocking component of routing device 10 can notice that the first packet is spoofed or that it cannot be acknowledged and ignore all other packets. Further, routing device 10 can use diagnostic detection tools (e.g., trace root, ping, NS lookup) to pinpoint attacker 16 and notify the system administrator. In general, according to the present invention, routing device 10 can be enabled to intelligently analyze incoming packets, match the packets against known patterns for attack strategies and respond accordingly to malicious packets.

FIGURE 2 is a flow chart of one embodiment of a method for blocking attacks on a private network according to the present invention. As shown, an incoming packet is analyzed by the routing device in step 20. In step 22, the routing device analyzes the incoming packet against known patterns. Based upon this pattern matching, in step 24, the routing device can identify the data packet and its source as malicious or non-malicious. The known patterns used in step 22 can be built using knowledge about various types of attacks. This knowledge can be recorded in the form of patterns that are then stored in a database or other storage device accessible by the routing device. The routing device can then match the analyzed packets against the patterns to determine whether or not some type of attack is being made. If an attack is identified, the routing device can identify the source of that packet as malicious and treat the source accordingly.

In particular, the routing device can implement methods for blocking denial of service attacks and address spoofing attacks as shown, for example, in FIGUREs 3 and 4. FIGURE 3 is a flow chart of one embodiment of a method for blocking an address spoofing attack according to the present invention. This method is applicable to address spoofing attacks on various types of networks, but is described speficially with respect to an IP network.

As shown in step 30 of FIGURE 3, the routing device receives a packet. In step 32, the routing device compares the IP address of the packet against known internal IP addresses of the associated private network. In step 34, the routing device determines if the source IP address matches an internal address. If not, in step 36, the routing device routes the packet as appropriate for the packet. However, if the source IP address matches an internal address, then the routing device identifies that there is an attempt to spoof an internal address. The addressed is known to be spoofed because an internal IP address of the private network cannot be accessing the private network from an external point. Consequently, in step 38, the routing device drops the packet and does not route it to the network. In step 40, the routing device analyzes the packet header for the history of the packet in order to obtain some information about the source of the packet. Then, in step 42, the routing device takes an appropriate defensive action against that packet. For example, the routing device can refuse to accept any more packets from the real source of the packet. In this case, the defensive action can include adding the offending IP address to a cache of IP addresses and then not allowing access to the router device for any IP address in the cached list. Further, the routing device can store information about the attack for later use and for analysis for administrators of the private network. For example, information concerning the packet origination, destination or content can be stored internally to the router device or sent to a syslog server for later analysis.

FIGURE 4 is a flow chart of one embodiment of a method for blocking a denial of service attack according to the present invention. As shown, in step 50, the routing device receives a request for a connection. Then, in step 52, the routing device asks for an acknowledgment from the requestor. In step 54, the routing device checks whether or not an acknowledgment has been received. If one is not received within a specified period of time, the routing device moves to step 56 and denies the request. This denial ensures that the routing device does not churn on pending requests even though acknowledgments have not been received within reasonable amounts of time.

If an acknowledgment is received in step 54, the routing device moves to step 58 and compares the requested connection to existing connections. Then, in step 60, the routing device determines if there is a match between the requested connection and one of the existing connections. If so, the routing device moves to step 46 and denies the request. The request is denied because one source should not have more than one connection through the routing device to the private network. If, in step 60, there is no match, then the routing device can allow the connection in step 62. The method of FIGURE 4 prevents the routing device from being tied up by multiple requests from one source and thereby blocks the denial of service attack.

In general, the method of the present invention can be integrated as a component of a gateway, firewall or other routing device. In one implementation, the present invention can work off of a variable size cache file that holds network addresses. For blocking spoofing, each incoming address can be held in the cache file and checked to see if the incoming address matches an network address that is on the private network. If the incoming address matches, then the request can be denied. Also, a message can be sent to a system log which, rather than being written to a file, can be written to a console to prevent the log from getting overloaded and crashing the routing device. Further, an optional E-mail message or page can be sent to a specified address or number in the case of an attack. If an attack happens more than once on the same address in the span of a certain period of time (for example, five minutes), then the number of messages can be limited to prevent overloading of the E-mail or paging service. An optional shutdown mechanism can also be in place that will enable the routing device to automatically shut down certain services if attacks continued.

Denial of service attacks are generally easier to trace. However, when such an attack is also spoofed, the problem becomes very difficult to stop. According to the present invention, an incoming address can be checked against the cache file and a quick search can be performed to see if the address is already in a list of pending addresses. If so, the request packet can be discarded. An address is removed from the list if a successful acknowledge packet is sent back or a variable time limit is reached. The number of matching addresses that are allowed in the list can be a variable set by the system administrator.

Although the present invention has been described in detail, it should be understood that various changes, substitutions and alterations can be made thereto without departing from the sphere and scope of the invention as defined by the appended claims.

WHAT IS CLAIMED IS:

1. A method for blocking attacks on a private network implemented by a routing device interconnecting the private network to a public network, comprising:

analyzing an incoming data packet from the public network;

matching the incoming data packet against known patterns, the known patterns associated with known forms of attack on the private network; and

identifying a source of the data packet as malicious or non-malicious based upon the matching.

2. The method of Claim 1, wherein one of the known forms of attack is a denial of service attack and an associated known pattern is unacknowledged data packets.

3. The method of Claim 1, wherein one of the known forms of attack is an address spoofing attack and an associated known pattern is a data packet having a source address matching an internal address of the private network.

4. The method of Claim 1, wherein the public network is the Internet.

5. The method of Claim 4, wherein the routing device is a firewall providing access to the Internet.

6. A method for blocking an address spoofing attack on a private network implemented by a routing device interconnecting the private network to a public network, comprising:

receiving an incoming data packet from the public network;

comparing a source address of the data packet against known internal addresses of the private network;

determining if the source address matches a known internal address;

if there is no match, routing the data packet to the private network;

if there is a match, dropping the data packet.

7. The method of Claim 6, further comprising, if there is a match, analyzing a header of the data packet for a history of the data packet and taking defensive action against the data packet based upon the history.

8. The method of Claim 7, wherein the defensive action comprises refusing to accept any more data packets from a real source of the data packet.

9. The method of Claim 7, wherein the defensive action comprises storing information about the data packet for use and analysis by a system administrator.

10. The method of Claim 6, wherein the public network is the Internet.

11. The method of Claim 10, wherein the routing device is a firewall providing access to the Internet.

12. A method for blocking a denial of service attack on a private network implemented by a routing device interconnecting the private network to a public network, comprising:

receiving a request for a connection from the public network;

requesting an acknowledgment from an initiator of the request;

determining whether an acknowledgment has been received;

if an acknowledgment is not received, denying the request;

if an acknowledgment is received, comparing the request to existing connections;

if there is a match between the request and an existing connection, denying the request;

if there is not match between the request and an existing connection, allowing the connection and routing packets to the private network.

13. The method of Claim 12, wherein the public network is the Internet.

14. The method of Claim 13, wherein the routing device is a firewall providing access to the Internet.

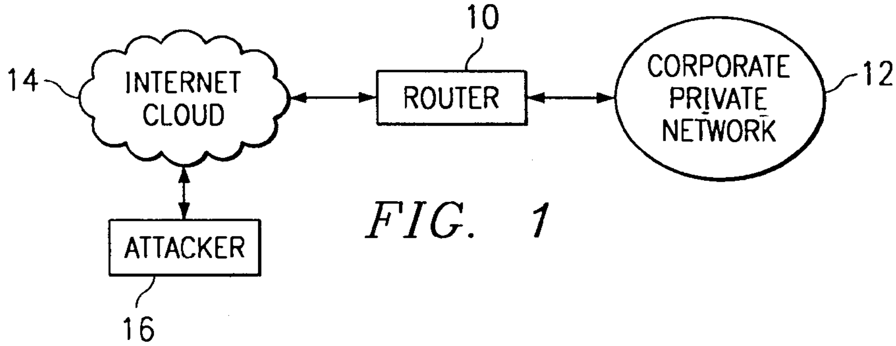


FIG. 1

FIG. 2

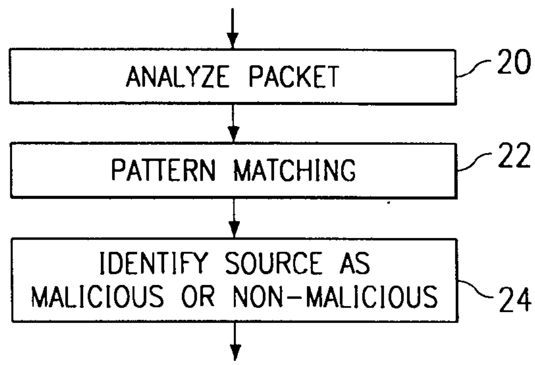


FIG. 3

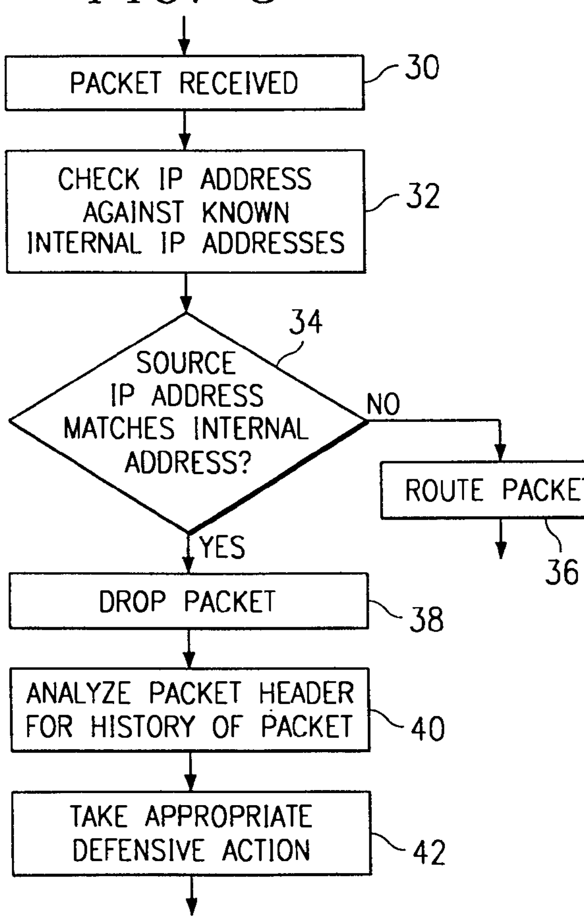
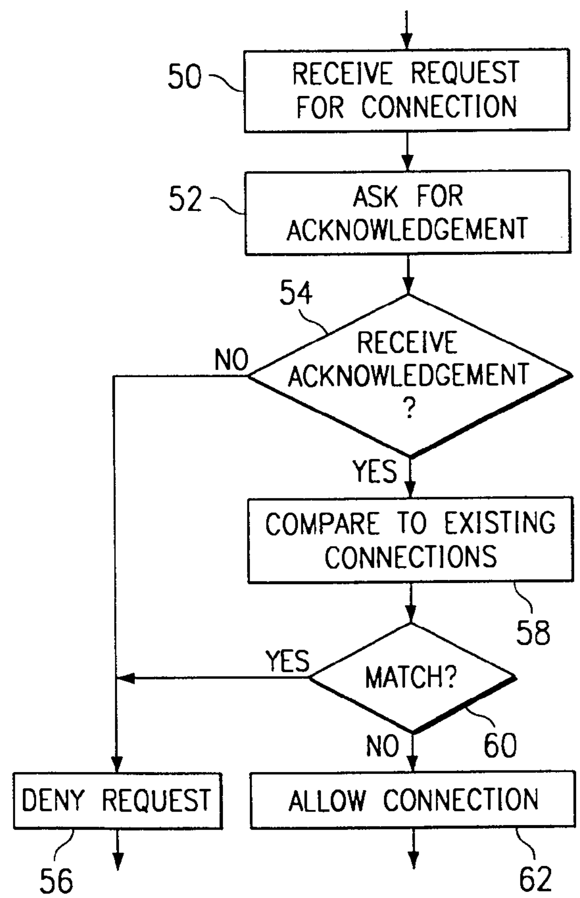


FIG. 4



Electronic Acknowledgement Receipt

EFS ID:	9448908
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN
Receipt Date:	15-FEB-2011
Filing Date:	16-AUG-2007
Time Stamp:	15:08:32
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	IDS.pdf	481967 e6b268dd0d9fd331f11f03f7bda54c3591b03cbe	no	10

Warnings:

Information:

This is not an USPTO supplied IDS fillable form					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
2	NPL Documents	Swan.pdf	255659 afccd65f57ba22dadb72048757c2f47b0f5a9b78	no	4
Warnings:					
Information:					
3	NPL Documents	Jones.pdf	206765 1573dedd590933d2f096947bfe92aa765a3d5fa4	no	15
Warnings:					
Information:					
4	NPL Documents	Wells.pdf	63145 095ce48eaedeaf4359dd456e88732c1e895de5e3	no	1
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
5	NPL Documents	Srisuresh.pdf	821507 57d3280aef2d3ae3b4a579021989331e0d16291e	no	28
Warnings:					
Information:					
6	NPL Documents	ISR13261.pdf	299844 f32c2c93b8fa7465ae3b37beb08f3731dce9d2ce	no	8
Warnings:					
Information:					
7	NPL Documents	ISRPCTUS99025323.pdf	138031 3d4cd666baae720c984c79205472c8535b7a6f1a	no	3
Warnings:					
Information:					
8	NPL Documents	ISRPCTUS99025325.pdf	141886 2fd71d5653d4fc8a333aa7a5a65213dde2a53ef9	no	3
Warnings:					
Information:					
9	NPL Documents	Reiter.pdf	344253 1dc436f7efb93d0ea624bc34abc9e7ef24afd8a7	no	23
Warnings:					
Information:					

10	NPL Documents	RFC2401.pdf	5794718 a633371efd69febe4083d1fac3a95eb7d526c430	no	66
Warnings:					
Information:					
11	NPL Documents	RFC2543.pdf	11969475 ddd10aa02dd5f96d70f69a01ca2f02edf773631c	no	153
Warnings:					
Information:					
12	NPL Documents	Rubin.pdf	5997094 fef9524ec8516987b9cbc8aad86460fc2b404d1c	no	15
Warnings:					
Information:					
13	NPL Documents	IPER04340.pdf	199081 7c0c52dd2e9cbc696d8c725497ba3a0b1981ac03	no	2
Warnings:					
Information:					
14	NPL Documents	ISR13260.pdf	246546 e495beedb0638e0a94c36b451b64cbd54272291e	no	8
Warnings:					
Information:					
15	NPL Documents	IPER13260.pdf	643372 f1a33d0d6b14bc636bbc227ca2119a2b0ba09480	no	7
Warnings:					
Information:					
16	NPL Documents	ISR04340.pdf	263704 8366e6e44abbc9f84817bd49410fc3deb562a086	no	7
Warnings:					
Information:					
17	NPL Documents	Shankar.pdf	637179 1e1ea1c65f6a0e94c1263144e966091b96eb9827	no	8
Warnings:					
Information:					
18	NPL Documents	Shree.pdf	9207540 b209fd155fdf36c73fe2e93e51cd5be192437209	no	9
Warnings:					
Information:					

19	NPL Documents	Transcript3810Afternoon.pdf	473103 71a99540889d09ea542389ff1debd8e3ccec675b	no	151
Warnings:					
Information:					
20	NPL Documents	Transcript3810Morning.pdf	371332 7d565afc267925e4e7888dc32bde6c9e61809933	no	119
Warnings:					
Information:					
21	NPL Documents	Transcript3910Afternoon.pdf	496076 3978812c01cdd7ee0840769d632718e03e39b7a6	no	170
Warnings:					
Information:					
22	NPL Documents	Transcript3910Morning.pdf	421929 9a4c23ad59cc9d0c2642d1240051056187422563	no	131
Warnings:					
Information:					
23	NPL Documents	Transcript31010Afternoon.pdf	557496 77182e5b350291ef09e41df738360df5a5d1fd45	no	191
Warnings:					
Information:					
24	NPL Documents	Transcript31010Morning.pdf	398144 6aa135e6a22e92ec32af3f2f6c62872f0825979f	no	125
Warnings:					
Information:					
25	NPL Documents	Transcript31110Afternoon.pdf	571904 134c2bc8606058f0fee7be5b9555e224f7514055	no	178
Warnings:					
Information:					
26	NPL Documents	Transcript31110Morning.pdf	350449 999d42732e60cfd94507a8cd114e95e61675c77f	no	120
Warnings:					
Information:					
27	NPL Documents	Transcript31210Afternoon.pdf	545435 fcf8d2e98d23cf06da7a7718156318448625290e	no	167
Warnings:					
Information:					

28	NPL Documents	Transcript31210Morning.pdf	430911 dbbb6593395ef47bb6539fc0cb16be7bfd6bd5ba	no	131
Warnings:					
Information:					
29	NPL Documents	Transcript31510Afternoon.pdf	693471 f9ba4bc92494c9aeb252fa67d3a058a363b8cb36	no	203
Warnings:					
Information:					
30	NPL Documents	Transcript31510Morning.pdf	514813 e6c7b4b57d1860f3c59e1537adabb2f9d4a52087	no	153
Warnings:					
Information:					
31	NPL Documents	Stallings.pdf	1451887 b32ca3a1d283b7ceeadc81e075be896ce51656dd	no	42
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
32	Foreign Reference	DE19924575.pdf	1465169 f29a1b60cadb9b76345bdb1fe79d4bcfbdab6f3d	no	15
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
33	Foreign Reference	EP0858189A3.pdf	191672 07cbac25a721f69c046c1dfd240be0ae1a488bab	no	6
Warnings:					
Information:					
34	Foreign Reference	EP0836306.pdf	1181950 64509eaea8cb2638c08c1ef0f9a1fdcbfdc2ee9e	no	15
Warnings:					
Information:					
35	Foreign Reference	WO0150688A1.pdf	1604707 cd89a9c972c6e3d7d424cc16c90e50479a7f79c6	no	37
Warnings:					
Information:					

36	Foreign Reference	WO9855930A1.pdf	1511981 3aa98dd038d7fdbc75f904e0db68ff5d1f18f206	no	28
Warnings:					
Information:					
37	Foreign Reference	WO9859470A3.pdf	164410 da8d2378929375d2208e4dd1ccff803a547062b2	no	5
Warnings:					
Information:					
38	Foreign Reference	WO99038081.pdf	1450345 4add54b10ef5943d00364f7d4f9f7a23931f0366	no	42
Warnings:					
Information:					
39	Foreign Reference	WO9948303A2.pdf	591963 8f63849cbcc9eeefeba1ae67bc4f94ca85e0127d	no	15
Warnings:					
Information:					
		Total Files Size (in bytes):	53150913		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

.Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** ***(Use as many sheets as necessary)***	**Complete if Known**	
	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1044	5,590,285	12/31/19996	Krause et al.	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 –Number 4 –Kind Code5 (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	C9	WO9843396	10/01/1998	Northern Telecom Limited			

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D81	European Search Report dated January 24, 2011 from corresponding European Application Number 10011949.4	
	D82	European Search Report dated March 17, 2011 from corresponding European Application Number 10184502.2	
	D83	Hollenbeck et al., “Registry Registrar Protocol (RRP) Version 1.1.0; Internet Engineering Task Force, 34 pages (1999)	
	D84	Notice of Allowance dated March 14, 2011 from corresponding US Application Number 11/840,508 (Our Ref. No.077580-0057)	
	D85	Tannenbaum, “Computer Networks,” pages 202-219 (1996)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** ***(Use as many sheets as necessary)***				**Complete if Known**	
				Application Number	**11/839,987**
				Filing Date	**08-16-2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2453**
				Examiner Name	**Lim, Krisna**
				Docket Number	**077580-0066**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[X] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

/Hasan M. Rashid/

Date: March 29, 2011

Hasan M. Rashid; Reg. No.: 62,390
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 27925972-1.077580.0066

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 12/66, H04Q 11/04

A1

(11) International Publication Number: WO 98/43396

(43) International Publication Date: 1 October 1998 (01.10.98)

(21) International Application Number: PCT/CA98/00197

(22) International Filing Date: 11 March 1998 (11.03.98)

(30) Priority Data:
08/821,145 20 March 1997 (20.03.97) US

(81) Designated States: AU, CA, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

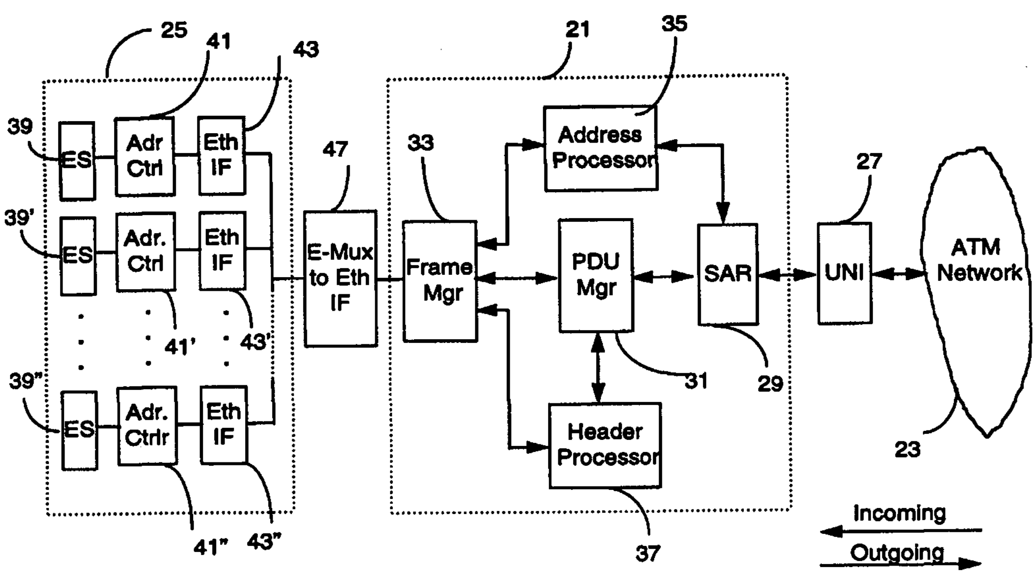
Published
With international search report.

(71) Applicant: NORTHERN TELECOM LIMITED [CA/CA]; World Trade Center of Montreal, 8th floor, 380 St. Antoine Street West, Montreal, Quebec H2Y 3Y4 (CA).

(72) Inventors: ALLAN, David, Ian; 852 Forest Street, Ottawa, Ontario K2B 5P9 (CA). CASEY, Liam, M.; 61 Aylmer Avenue, Ottawa, Ontario K1S 2X2 (CA). ROBERT, Andre, J.; 103 Sol Lane, R.R. #2, Woodlawn, Ontario K0A 3M0 (CA).

(74) Agent: DIACONESCU, Aprilia, U.; Northern Telecom Limited, Patent Dept., P.O. Box 3511, Station "C", Ottawa, Ontario K1Y 4H7 (CA).

(54) Title: A MECHANISM FOR MULTIPLEXING ATM AAL5 VIRTUAL CIRCUITS OVER ETHERNET



(57) Abstract

The invention provides for an E–Mux and a method for encapsulating/segmenting ATM cells into/from an Ethernet frame at the boundary between an ATM and an Ethernet network. An Ethernet end–station on the E–Mux is addressed using multiple MAC level identifiers, which are dynamically assigned according to the ATM virtual circuits which terminate on that end station, and have only transitory significance on the Ethernet. A unique ATM OUI identifies the frames carrying ATM–traffic.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

A MECHANISM FOR MULTIPLEXING ATM AAL5 VIRTUAL CIRCUITS OVER ETHERNET

Field of the Invention

The invention is directed to a system and method for carrying ATM network information over a local area network (LAN), and more particularly to a mechanism for multiplexing ATM AAL5 virtual circuits over Ethernet.

Background of The Invention

The asynchronous transfer mode (ATM) forms the basis for switching in broadband networks. ATM is a connection oriented data transport which is media independent. The key feature of ATM is the segmentation of data into fixed length units of data referred to as cells. Each cell is separately steered at each ATM switch via an identifier of local significance to the local transport leg provided in the header of each cell. The identifiers are reassigned during the transit of a cell from an input port to an output port on a switch. The identifier carried between a switch and an end system is 24 bits in length. For an ATM user network interface (UNI), this is a concatenation of a 16 bit virtual circuit identifier (VCI) and an 8 bit virtual path identifier (VPI).

This routing mechanism differs significantly from other networks, in that there is only one identifier specifying a local path vs. source and destination information. This path information in itself is insufficient to uniquely identify the real source and destination for the payload and therefore the connection is set up via signalling. As such, connection to a remote end-station is requested and upon connection set-up, the network informs the end station what the local identifier of the connection is.

Ethernet is a connectionless LAN technology designed for data applications in which all stations on the network share the communication medium. This medium, which could be twisted pairs, fiber, or coaxial cables, is shared in a peer to peer fashion. All devices on the Ethernet can be reached by a single transmission of data. Ethernet operates typically at 10Mbs and the data are sent in the form of Ethernet "frames".

There is no central arbitrator of bandwidth to administer media access on an Ethernet. Every time an Ethernet end station sends message, it listens to the media to ensure that it is not in use by another station. If this is true, the end station commences sending its own message. During the message send phase, the end station monitors the media to detect if another station has also commenced sending at the same time. The minute delays imposed by the speed of light permit a relatively large window wherein multiple stations can believe that the media is idle, and therefore can commence sending an Ethernet frame. If the end station detects a collision, i.e. what it hears does not match what it sends, it switches to sending a short "jabber" sequence to ensure that all colliding end stations detect that contention has occurred. All end-stations detecting a collision will wait a random interval and will then retry sending their frame, once again applying the same rules to determine success, and to free up the channel as quickly as possible when a collision occurs. Additional error detection is built into each frame to ensure that errored frames are not propagated.

Ethernet end stations are addressed globally and uniquely by a 48 bit media access control (MAC) address. The MAC address is comprised of a 24 bit Organization Unique Identifier (OUI) and a 24 bit end station identifier (ID). OUI is a globally administered numbering plan which comprises a portion of a number identifying the organization administering the remainder of the number, which is IEEE for Ethernet. The ID is a unique identifier that a manufacturing organization can provide to all equipment that it manufactures. Further, this identifier is unique and staticaly assigned and well known to the station. Certain Ethernet addresses are reserved for broadcast and multicast to all end-stations on the segment and for diagnostic purposes.

An Ethernet connected end station receives all data broadcast onto the media. By convention, the end station discards all traffic not directed to itself, all, or a subset of end stations, as identified in the destination MAC address.

All major emerging communication technologies rest on the layers of the OSI model. The OSI model defines a physical layer which specifies the standards for the transmission medium, a data link layer (layers 2 and 3) and a network layer (layers 4 to 7). Thus, in many cases, Ethernet operates on FDDI (fiber distributed data interface) physical layer, and the MAC layer, placed on top of FDDI, comprises the data layer. ATM operates on SONET, copper, twisted pairs, FDDI as physical layer, and the data layer is subdivided into an ATM layer and an ATM adaptation layer (AAL) providing the convergence function (called also convergence sublayer CS). Whatever the implementation of the AAL at the UNI, the ATM network is not concerned with the AAL operations, the ATM bearer service is masked from the convergence function.

It has become evident that LAN shared bus architecture is insufficient to meet the demands of applications that require more bandwidth, and that LANs are beginning to become a bottleneck in computing environments. For this reason, more economic local interfaces such as a Frame-Relay version (FUNI) and an Ethernet version, Cells-in-Frames (CIF), are used in the access network. In both cases, the separation of data into cells is deferred until within the network, but the higher level information is carried to the end station. In addition, according to the CIF version the AAL5, PDUs are pre-packaged at the end station and this implies changes in HW and SW at each Ethernet connected end station.

Switched Ethernet technology, developed to provide more capacity to an end-user, does not relay on shared medium, it rather provides point-to-point bandwidth between the user station and the switch, so that instead of sharing a 10 Mbit/s medium, the user gets a dedicated 10 Mbits/s medium. As Ethernet hubs and switches are growing in use, they become an inexpensive means to provide more bandwidth to workstations. A switched Ethernet network is more flexible, in that it may include stations that are using a port at a given full rate, stations that share a port, or stations that have access to more than one port.

However, switched Ethernet provides only limited bandwidth and supports data traffic only. A more efficient solution for bursty traffic is needed. There is also a need to simplify and standardize the access link while also obtaining protection of the access traffic.

Although ATM provides a very rich environment with numerous traffic classes and the ability to multiplex many data streams with different handling requirements together, this functionality is mainly required in the network backbone. It is sought that ATM networks will be used by more general class end stations for delivering multi-media services. However, in the short term, the extra bandwidth and cost of ATM interfaces is probably not justified for general class end stations, such as desktop computers. It is possible to built ATM switches with lower speed ATM interfaces, but this solution presents a serious deployment problem in that it requires replacement of the substantial installed base of shared media LAN wiring and adapter cards.

An ATM-Ethernet concentrator is disclosed in United States Patent No. 5,457,681 (Gaddis et al., issued on October 10, 1995 and assigned to Washington University), which provides an interface between an ATM network and a plurality of Ethernet segments. Each Ethernet frame transmitted by any of the Ethernet segments is fragmented into a sequence of ATM cells, which are transmitted by an Ethernet controller associated with the respective segment over the ATM network and delivered to the interconnected Ethernet controllers. When the cells are received, the controller re-assembles them into frames and transmits the frames over the respective Ethernet segment to the end stations. While this patent partially addresses the problems of bandwidth and cost, it does not provide a method and system for transmitting ATM cells in Ethernet frames, for taking advantage of the ATM capabilities.

There is a need to provide an improved network communication system with minimal displacement of existing network components, capable of providing large bandwidth to the end stations for data, video and voice traffic, and providing LAN access to switched point-to-point WAN links.

International application No. PCT/CA95/00029 (WO 95/20282) (by Burwell et al. published on July 27, 1995 and assigned to Newbridge Networks Corporation) discloses a communication network comprising ATM switches interfaced with LANs, the ATM cells being encapsulated in LAN frames and being delivered in encapsulated form over the Ethernet LAN direct to the end station. In another embodiment, the LAN interface adapter of the end station provide bridging, network layer functions and LAN emulation functions to permit transparent communication between the end stations over the ATM network. The interface adapter, also defined as a "ridge (bridge/router) creates frames from ATM cells and vice-versa.

However, the method disclosed in the above patent layers ATM carriage on top of the Ethernet layer. This is to say, ATM information only appears within the Ethernet payload, imposing an extra layer of indirection and frame processing on ATM handing at the LAN/WAN boundary.

Summary of the Invention

It is an object of this invention to provide a mechanism for transmitting ATM cells in Ethernet frames for interworking of ATM backbone networks with the large base of legacy equipment, and for re-establishing access to an ATM network for a LAN.

It is another object of the invention to provide an addressing convention for carriage of ATM over Ethernet to a specified end station.

This invention is based on the fact that although an Ethernet MAC address is normally globally unique for universal interoperability, it does not absolutely have to be for a closed Ethernet to work. Uniqueness of the address within the Ethernet broadcast domain itself is necessary. According to this invention, an Ethernet end station is allowed to assume multiple MAC level identifiers on a single Ethernet interface. These identifiers which are dynamically assigned, have only transitory significance on the Ethernet.

Accordingly, the invention provides a multiplexer (E-Mux) for encapsulating ATM cells into a LAN frame, comprising a segmentation and reassembly unit for receiving a plurality of incoming ATM cells with a LAN destination address and generating an ATM adaptation layer 5 (AAL5) protocol data unit (PDU); a PDU manager for receiving the AAL5 PDU and extracting an AAL5 payload; a header processor for extracting a traffic type indicator from the header of the PDU; an address processor for extracting the LAN destination address from the header of an incoming ATM cell; and a frame manager for receiving the traffic type indicator, the AAL5 payload and the LAN destination address and generating an incoming LAN frame.

The invention also provides a multiplexer (E-Mux) for segmenting a LAN frame into a plurality of ATM cells, comprising: a frame manager for receiving an outgoing LAN frame with an ATM destination address and de-assembling it into a traffic type indicator, an AAL5 payload and an ATM destination address; a header processor for receiving the traffic type indicator from the frame manager; a PDU manager for receiving the AAL5 payload and the traffic type indicator and generating an ATM adaptation layer 5 (AAL5) protocol data unit

(PDU); an address processor for receiving the ATM destination address from the frame manager; and a segmentation and reassembly unit for receiving the PDU and the ATM destination address generating a plurality of ATM cells with the ATM destination address.

According to another aspect of the invention, there is provided a telecommunication network comprising a LAN with a plurality of end-stations connected over a transmission medium and an ATM network, comprising: a multiplexer (E-Mux) for encapsulating a plurality of ATM cells received from the ATM network into an incoming LAN frame and for segmenting a LAN frame received from the LAN network into a plurality of outgoing ATM cells; an E-Mux-to-LAN interface for adapting the transmission format of the LAN frame for transmission over the connection medium of an LAN network; an ATM-to-E-Mux interface for adapting the transmission format of the ATM cells received from an ATM network for processing by the E-Mux; an address controller at each end station for forwarding the incoming LAN frame to the end station when a destination address comprised in the destination MAC field of the LAN frame is recognized by the address controller, and for inserting an ATM destination address into the source MAC field of the outgoing frame.

A method for transmitting information from an ATM network to an Ethernet network using an E-Mux is also disclosed, the method performing the steps of: establishing connection between an ATM switch of the ATM network and an end station of the Ethernet network based on a VPI/VCI destination address in the header of an incoming ATM cell; receiving a plurality of incoming ATM cells with the destination address, and generating an ATM adaptation layer 5 (AAL5) protocol data unit (PDU) with a segmentation and reassembly unit; extracting an AAL5 payload from the PDU with a PDU manager; extracting a traffic type indicator from the header of the PDU with a header processor; generating with a frame manager an incoming Ethernet frame using the traffic type indicator, the AAL5 payload and the destination address; and transmitting the Ethernet frame over the Ethernet network to the end station according to the destination address.

According to still another aspect of the invention, there is provided a method for transmitting information from an Ethernet network to an ATM network using an E-Mux performing the steps of: establishing connection between an end station of the Ethernet network and an ATM switch of the ATM network based on a VPI/VCI destination address provided by the end station; generating an outgoing Ethernet frame at the end station and transmitting same to the E-Mux; extracting from the Ethernet outgoing frame a traffic type indicator, a frame payload and a source address, with a frame manager; generating an ATM adaptation layer 5 (AAL5) protocol data unit (PDU) with a segmentation and reassembly unit from the frame payload and a traffic type indicator extracted from the type field of the outgoing frame with a header processor; segmenting the PDU into a plurality of outgoing ATM cells and inserting a VPI/VCI destination address in the header of the cells from an address processor.

Advantageously, the system and method of the invention provides a highly efficient carriage of ATM information to an end station using actual MAC address space in the Ethernet frame.

Because the frames are not pre-packaged into AAL5 PDUs at the end station, but at the E-Mux, the system of the invention is efficient, as custom hardware to perform this function does not need to be deployed at each Ethernet connected end station, and the end station software is not burdened with this task. Custom hardware to perform SAR (segmentation and reassembly) function is built into the E-Mux.

Still another advantage of the invention is that legacy Ethernet can coexist with ATM LAN to UNI traffic. ATM intelligence can be distributed in such a LAN segment. For meshed PVC/UBR type connections, standard packet formats and driver interfaces may be used between layer 3 and the Ethernet interface, making the invention applicable to various LAN technologies. No additional information needs to be propagated outside the system of the invention. Therefore, this permits the system to be tailored as an application specific ATM to Ethernet interface.

Still another advantage of the invention is that the Ethernet frame is efficiently used since the ATM routing information is embedded in the Ethernet MAC addressing field. No additional ATM header within the Ethernet payload is necessary, since the entire ATM semantics is not carried to the end station. This does not preclude, however, additional semantics being packaged in a separate header in the Ethernet frame.

ATM virtual circuit (VC) address mapping is carried forward into the Ethernet domain. Intermediate steps are not required to map Ethernet MAC to VC, as VC information flows end-to-end. For uncommitted bit rate (UBR) data services, only the ATM path identifier need to be carried forward across an Ethernet LAN.

As a result, Ethernet traffic can coexist-exist with ATM LAN to UNI traffic. As indicated above, each Ethernet connected station may assume multiple IDs on the LAN at the MAC level. Thus, for traditional, non-ATM traffic, it retains the manufacturers MAC address built into the Ethernet interface at the factory. For ATM traffic, it assumes one or more IDs depending on the ATM virtual circuits which ultimately terminate at that particular end station interface.

Brief Description of the Drawings

The foregoing and other objects, features and advantages of the invention will be apparent from the following more particular description of the preferred embodiments, as illustrated in the appended drawings, where:

Figure 1A shows the convergence and segmentation and reassembly functions of ATM (prior art);

Figure 1B shows an ATM network for defining the terms virtual channel and virtual path (prior art);

Figure 1C shows an Ethernet frame (prior art);

Figure 2 shows the block diagram of the E-Mux;

Figure 3A shows the processing of the ATM cells to produce an incoming Ethernet frame;

Figure 3B shows the processing of an outgoing Ethernet frame to produce ATM cells;

Figure 4A is a the flow-chart illustrating the assembly of the ATM cells to produce an Ethernet frame;

Figure 4B is a the flow-chart illustrating the segmentation of the Ethernet frame to produce ATM cells;

Figure 5 shows the block diagram of a variant of the E-Mux;

Figure 6A shows the processing of the ATM cells to produce an incoming Ethernet frame according to the variant of Figure 5; and

Figure 6B shows the processing of an outgoing Ethernet frame to produce ATM cells according to the variant of Figure 5.

Description of the Preferred Embodiment

Figures 1A, 1B, and 1C are provided for defining and illustrating some of the terms necessary for describing the present invention and its mode of operation.

Figure 1A shows the convergence function, and the segmentation and reassembly (SAR) function of ATM. The convergence function is responsible for accepting the user traffic which could range from one to maximum 65,000 bytes, and placing a header **10** and a trailer **12** around it to obtain a protocol data unit (PDU) **2**. For this invention, the payload field of the PDU is limited to 1,500 bytes, which is the size of the Ethernet payload field. To push PDU beyond Ethernet limit of 1,500 bytes will require an additional header in the Ethernet frame. The length of the header and trailer is between 6 and 40 bytes. Once the header and the trailer have been added to the user payload, the traffic is segmented into 44-48 bytes data units **14**. Next, the adaptation layer adds a header **16**, and possibly a trailer **18** to the data unit **14**, depending on the type of payload being supported. In any event, the final data unit from this operation is always a 48 octet block **20**. Finally, the last operation is performed by the data link layer which adds a five-octet header **22** to the 48-octet payload **20** resulting in a 53 bytes cell **24**. Each cell is transported over the physical layer between two ATM switches designated by the address information in header **22**.

Figure 1B shows a basic linear point-to-point ATM network configuration where the connections are identified through virtual channel identifiers (VCI) and virtual path identifiers (VPI) in the ATM cell header. Switching in the ATM network is illustrated at **5**, **7**, and **9**. A virtual channel connection (VCC) **11** has end-to-end significance between end users A and B. A virtual path connection (VPC) has significance between adjacent ATM devices, **5**, **7**, and **9**, and switching is performed very quickly through the use of a routing table.

Figure 1C illustrates an Ethernet frame. Ethernet end stations are addressed globally and uniquely by the MAC address. Field **28** comprises the destination MAC and field **30** comprises the source MAC. The MAC address is has a 24 bit organizationally unique identifier (OUI) **38, 42** and a 24 bit end station identifier **40, 44**.

A type field **32** is provided for specifying the traffic type.

The payload field **34** may comprise up to 1500 bytes. The frame begins with a training sequence **26** for allowing receiver synchronization and ends with a frame check sequence **36**, for determining the integrity of the data in the frame.

Figure 2 shows the block diagram of the system according to the invention. An E-Mux **21** exchanges ATM cells with an ATM UNI **27**, which is connected in turn to an ATM network **23**. E-Mux **21** is also connected to an Ethernet LAN **25** for exchanging frames. By convention, the traffic travelling from ATM network **23** to LAN **25** is defined by the term "incoming", and the traffic travelling from LAN **25** to ATM network **23** is defined by the term "outgoing".

According to the invention, a unique MAC OUI is established for extending ATM path addressing into the Ethernet MAC address domain. This unique MAC OUI identifies the traffic as ATM UNI. The ATM OUI is inserted in both the destination and the source MAC fields **38** and **42**. The OUI field informs LAN **25** that the traffic is coming from a source not registered to it, so as to treat it accordingly. As indicated earlier, this permits the ATM traffic to coexist with traditionally addressed Ethernet traffic.

E-Mux **21** associated to LAN **25** also requires a unique ID in the destination MAC, such that incoming traffic can be uniquely addressed to it. The ID could be for example VPI=0, VCI=0, which is never used in the ATM network **23**. This unique address, ATM OUI, VPI=0,VCI=0, is mapped into the source MAC field **30** of an incoming frame and in the destination MAC of an outgoing frame. This is described next in connection with Figures 3A, which shows the processing of the ATM cells to produce an incoming Ethernet frame and Figure 3B, which shows the processing of an outgoing Ethernet frame to produce ATM cells.

Each end station has an VPI/VCI address for the ATM traffic used to establish connection between a switch in the ATM network and an end station through signalling in a known manner. For the incoming traffic, a flow of cells **24**, addressed to an end station **39, 39', 39"** in Ethernet network **25** is received at UNI **27** from network **23**. The cells are assembled into a PDU **2** by SAR unit **29** of E-Mux **21**.

PDU **2** comprises a AAL5 payload field **14** for receiving the payload from the incoming cells **24**, the size of the payload field being limited to the maximum size of field **34** (up to 1500 bytes) of an Ethernet frame **3**. Although the normal ATM AAL5 protocol data unit (PDU) is quite large, as discussed in connection to Figure 1, it can be constrained to fit within the 1500 bytes of an Ethernet frame.

Since the size of the PDU is restricted to the payload field length of a frame, the cell segmentation function is performed by SAR **29** at boundary to the ATM network, such that the need for additional PDU information to be carried in the payload portion of the Ethernet frame is obviated. This differs from the cell-in-frame (CIF) approach in which the SAR function is performed at the end station, and then the cells are reassembled into Ethernet frames for transmission.

A PDU manager **31** strips the LLC/SNAP (Logical link control, sub-network attachment point) header of the PDU **2** and provides it to a header processor **37**, which determines the type of the payload. The payload and the payload type are forwarded to a frame manager **33**.

Frame manager **33** generates the Ethernet frame **3** by mapping the payload into field **34** and the payload type into field **32**. Frame manager **33** also receives the address of the destination end station from an address processor **35**, and maps this information into field **40** of destination MAC. This address is a concatenation of the VPI/VCI address extracted from the cell header **22**. As well, address processor **35** maps the address of the E-Mux in the source MAC field **30**, namely ATM OUI and VPI=0, VCI=0 in fields **40** and **42**, respectively. As such, for the incoming traffic, the source MAC field of frame **3** comprises the address of the E-Mux, and the destination MAC comprises the address of the end station in the Ethernet.

Frame manager **33** sends frame **3** assembled as indicated above, over the Ethernet network **25**. An interface **47** is provided for adapting the format of the frame to the connection medium of Ethernet 25.

In general, each "ATM aware" end station **39, 39', 39"** is provisioned with an address controller, as shown at **41, 41', 41"**, which allows the end station to signal the network to request/accept connections. As well, address controller **41, 41', 41"** provides the range of VPI/VCI values that could be assigned for such connections to the associated end station **39, 39', 39** to a defined subset of the whole VPI/VCIs allocated for UNI **27**. An address controller **41, 41', 41"** recognizes a destination ID as being its own, using a look-up table, and directs frame **3** to the associated end station **39, 39', 39"**.

For the outgoing direction, an end station **39, 39', 39"** generates an outgoing frame **3**, with the destination MAC indicating the ATM OUI address of E-Mux **21**, rather than the address of another end station in the Ethernet network **25**. As such, the corresponding Ethernet interface transmits the outgoing frame to E-Mux **21**. The source MAC ID field **44** comprises the VCI/VCI address, of the destination ATM device in ATM network **23**.

Now, frame manager **33** receives the frame from interface **47**, segments the frame and provides the payload to PDU manager **31**, the VPI/VCI address to address processor **35** and the type information from field **32** to header processor **37**. PDU manager **31** generates a PDU **2** by inserting the payload received from frame manager **33** into field **14**, and the type information from header processor **37** into LLC/SNAP header field **16**. PDU is then forwarded to SAR **29** which segments the PDU **2** into cells **24**, for UNI **27**. Address processor **35** inserts the VPI/VCI address from the source MAC ID field **44** into each cell header, so that ATM network **23** switches the cell accordingly.

A simple example of this technique would be that end station **39** has established an ATM connection on VCI=5, VPI=7. For all traffic that is to be directed beyond the Ethernet onto the ATM network **23**, end station **39** would set the destination MAC address in the Ethernet frame to that of the E-Mux **21**, which is ATM-OUI, VPI=0, VCI=0, and would identify the virtual circuit via the source MAC, which will show ATM-OUI, VPI=7, VCI=5, identifying the source as the owner of that VCC. Traffic flowing in the direction from E-Mux **21** to end station **39**, would see the source and destination addresses reversed.

As a simple extension of this concept, an Ethernet station, when originating signalling, may use the source MAC field for the normal Ethernet MAC and the destination MAC field for the ATM-OUI and '0'. The source MAC field permits an E-164 encoded NSAP to give the

Ethernet connected end station a unique identification in the ATM network. In this way, the E-Mux can arbitrate and aggregate signalling onto a standard UNI from multiple Ethernet connected devices.

Additional overhead is eliminated by performing the ATM AAL5 protocol encapsulation at the E-Mux (e.g. normal protocol encapsulation for AAL5 as defined by RFC1483). Thus, an encapsulation of the cells into a PDU frame is effected by PDU manager **31**, and an encapsulation of the PDU into an Ethernet frame is effected by the frame manager **33**, such that the Ethernet end station does not have to be ATM protocol aware, or perform CRC (cyclic redundancy check) and SAR (segmentation and reassembly) functions.

Figure 4A is a the flow-chart illustrating the processing of the ATM cells to produce an Ethernet frame. In step **100**, a connection between the station in the ATM network and the E-Mux **21** is established based on the ATM address of the E-Mux. An address controller, lets say **41**, recognizes its associate end station as the owner of the VPI/VCI, and station **39** establishes communication with ATM network **2**, shown in step **110**.

When E-Mux **21** receives a flow of ATM cells over a specific VC, as shown in step **120**, it assembles the cells into a PDU, step **130**, verifies that the AAL5 **CRC** is correct, in step **140**, and maps the payload into the payload portion of the Ethernet frame in step **150**. The destination MAC is set in field **28** to ATM OUI, VCI/VPI in step **160** to uniquely identify the owner of that particular path on the LAN, and the source MAC is set to that of the E-Mux, namely ATM OUI 0x00, in step **170**.

The E-Mux broadcasts the Ethernet frame onto the Ethernet network in step **180**. Station **39** with ID VPI/VCI in the destination MAC receives the frame, while other stations **39'**, **39"** on the Ethernet, receive the frame and discard it as they are not addressed to them, as shown in step **190**.

Figure 4B shows a the flow-chart illustrating the processing of an Ethernet frame to produce ATM cells.

First, in step **200**, an end station, for example station **39** originates a message to be sent, for example, over VCI=5, VPI=7. It prepares an Ethernet frame as shown in Figure 3B directed to the E-Mux by inserting the ATM OUI in fields **38** and **42**, the VPI=0, VCI=0 address in the destination MAC field **40** and inserts the ATM virtual circuit address information in the source MAC address field **44**.

In step **210**, station **39** broadcasts the frame on the Ethernet. Other stations on the Ethernet receive the frame, check the destination MAC in step **220**, and discard it in step **230**, as they are not the addressed recipients of this frame.

E-Mux **21** receives the frame in step **240**, and as the recipient, keeps the frame. It performs ATM AAL5 PDU and SAR processing on the payload steps **250** and **260**, extracts the ATM virtual circuit address information from the frame source MAC and inserts it into the cells headers in step **270**. The resulting cells are transmitted in step **280** over the address specified by the VPI/VCI address information.

Additional processing could be performed during processing of the cells from the Ethernet frames. For example, an Ethernet II/DIX format frame could be converted to RFC1483 encapsulation prior to AAL5 and SAR handling as an additional interworking step.

The invention may be used for providing ATM WAN (wide area network) access from a LAN. This permits a LAN connected computer to establish unique and private WAN connections, while maintaining access to all legacy services deployed on the non-ATM aware portions of the local LAN.

Use of Ethernet networks as a distributed multiplexer backbone over several shelves of equipment, permits an Ethernet to be used as the media to demultiplex an ATM UNI over a collection of devices distributed over a large area (e.g. up to 6000 feet for 10BaseT). The typical application would see shelf and line card encoded in the ATM VPI/VCI addressing scheme to permit static de-multiplexing of the UNI.

A variation of the E-Mux of the invention can function as an ATM to Ethernet multiplexer, as shown in Figure 5.

This variant provides for a highly scaleable and optionally redundant UNI termination for IP (Internet Protocol). The automated association of IP to VCI/VPI can be utilized to produce ATM interfaces for IP protocol based devices which can support significantly more virtual circuits than are currently available. This eliminates the requirement for the address controllers **41, 41', 41"** residing in the attached end station **39, 39', 39"**. This also moves the IP->ATM association from the custom hardware in the Ethernet interface **43, 43', 43"**, to the traditional Ethernet ARP cache resident on the end station. Current ATM interfaces are limited to between 500 and 2000 VCs. This invention permits interfaces for relatively low bandwidth connections (as for an ATM based element management channel) to scale up to more than 50,000 virtual circuits.

In this case the E-Mux **50** assumes the OUI/VPI/VCI identifiers and the attached end station retains its normal MAC address. Figure 6A shows the processing of the ATM cells to produce an incoming Ethernet frame and Figure 6B illustrates the processing of an outgoing Ethernet frame to produce ATM cells, for E-Mux **50**.

For the incoming traffic source OUI field **42** contains the ATM OUI to indicate to the end station that traffic comes from the ATM network **23**. The VPI/VCI address form the cell header **22** is mapped by E-Mux **50** into the source ID field **44**. The destination MAC field **28** comprises the Ethernet MAC of the station recipient of the respective frame.

For the outgoing traffic, Figure 6B shows that the end station inserts the ATM OUI identification in field **38** of the destination MAC field **28** and the VPI/VCI address of the destination station in the ATM network **23** in field **40** of the destination MAC. The E-Mux **50** inserts the VPI/VCI address into the cell headers, so that the cells are switched accordingly in network **23**. The source MAC field **30** comprises the

Ethernet address of the end station in the Ethernet network that generated the respective frame.

There are numerous ways by which the embodiment of Figure 5 can learn the Ethernet MAC address of the attached end stations. Alternatively, the Ethernet all-stations broadcast address can be used.

The generalized operation is that an attached end station learns the IP->MAC association for devices remotely connected to the ATM network as it would for a normal Ethernet. However, the MAC addresses presented actually contain VPI/VCI information by which those devices can be reached. The attached host is "spoofed" into having an Ethernet layer 2 address mapping for ATM connected devices such that Ethernet address resolution and forwarding mechanisms make ATM attached devices reachable.

This invention can also be used to provide hot standby backup platforms. Normally an ATM connection is unique and cannot automatically be locally switched to another platform. The availability of Ethernet as a broadcast medium permits the ATM traffic to be fanned out to multiple devices simultaneously and only acted upon by the current "active" platform.

While the invention has been described with reference to particular example embodiments, further modifications and improvements which will occur to those skilled in the art, may be made within the purview of the appended claims, without departing from the scope of the invention in its broader aspect.

WE CLAIM:

1. A multiplexer (E-Mux) for encapsulating ATM cells into a LAN frame, comprising:

a segmentation and reassembly unit for receiving a plurality of incoming ATM cells with a LAN destination address, and generating an ATM adaptation layer 5 (AAL5) protocol data unit (PDU);

a PDU manager for receiving said AAL5 PDU and extracting an AAL5 payload;

a header processor for extracting a traffic type indicator from the header of said PDU;

an address processor for extracting said LAN destination address from the header of an incoming ATM cell; and

a frame manager for receiving said traffic type indicator, said AAL5 payload and said LAN destination address and generating an incoming LAN frame.

2. A multiplexer as claimed in claim 1, wherein said LAN is an Ethernet network and said incoming LAN frame is an Ethernet frame.

3. A multiplexer (E-Mux) for segmenting a LAN frame into a plurality of ATM cells, comprising:

a frame manager for receiving an outgoing LAN frame with an ATM destination address and de-assembling it into a traffic type indicator, an AAL5 payload and an ATM destination address;

a header processor for receiving said traffic type indicator from said frame manager;

a PDU manager for receiving said AAL5 payload and said traffic type indicator and generating an ATM adaptation layer 5 (AAL5) protocol data unit (PDU);

an address processor for receiving said ATM destination address from said frame manager; and a segmentation and reassembly unit for receiving said PDU and said ATM destination address generating a plurality of ATM cells with said ATM destination address.

4. A multiplexer as claimed in claim 3, wherein said LAN is an Ethernet network and said outgoing LAN frame is an Ethernet frame.

5. A multiplexer as claimed in claim 2, further comprising:

an E-Mux-to-Ethernet interface for formatting said Ethernet frame for transmission over the connection medium of an Ethernet network; and

an ATM-to-E-Mux interface for formatting said ATM cells received from an ATM network for processing by said E-Mux.

6. A multiplexer as claimed in claim 4, further comprising:

an E-Mux-to-ATM interface for formatting said ATM cells for transmission over the medium of an ATM network; and

an Ethernet-to-E-Mux interface for formatting said Ethernet frame received over a transmission medium of an Ethernet network for processing by said E-Mux.

7. An Ethernet network comprising a plurality of end stations and an Ethernet/ATM interface connected over a transmission medium, each end station comprising an address controller for forwarding an incoming LAN frame received from said Ethernet/ATM interface ATM network to said end station when a destination address comprised in the destination MAC field of said frame is recognized by said address controller, and for inserting an ATM destination address into the source MAC field of an outgoing frame destined to said Ethernet/ATM interface.

8. A telecommunication network comprising a LAN with a plurality of end-stations connected over a transmission medium and an ATM network, comprising:

a multiplexer (E-Mux) for encapsulating a plurality of incoming ATM cells received from said ATM network into an incoming LAN frame and for segmenting an outgoing LAN frame received from said LAN network into a plurality of outgoing ATM cells;

an E-Mux-to-LAN interface for formatting said incoming LAN frame for transmission over the connection medium of said LAN network, and for formatting said outgoing Ethernet frame received over the connection medium of said LAN network for processing by said E-Mux;

an ATM-to-E-Mux interface for formatting of said incoming ATM cells received from said ATM network for processing by said E-Mux, and for formatting said outgoing cells for transmission over the medium of said Ethernet network; and

an address controller at each end station for forwarding said incoming LAN frame to said end station when a destination address comprised in the destination MAC field of said incoming LAN frame is recognized by said address controller, and for inserting an ATM destination address into the source MAC field of said outgoing LAN frame, when said outgoing LAN frame is destined to said ATM network.

9. A method for transmitting information from an ATM network to an Ethernet network using an E-Mux performing the steps of:

establishing connection between an ATM switch of said ATM network and an end station of said Ethernet network based on a VPI/VCI destination address in the header of an incoming ATM cell;

receiving a plurality of incoming ATM cells with said destination address, and generating an ATM adaptation layer 5 (AAL5) protocol data unit (PDU);

extracting an AAL5 payload from said PDU;

extracting a traffic type indicator from the header of said PDU;

generating an incoming Ethernet frame using said traffic type indicator, said AAL5 payload and said destination address; and

transmitting said Ethernet frame over said Ethernet network to said end station according to said destination address.

10. A method as claimed in claim 9, wherein said incoming Ethernet frame comprises:

a destination MAC field including:

a unique ATM OUI identifier indicating that said incoming Ethernet frame comprises ATM traffic; and

said VPI/VCI destination address specifying the address of said end station;

a source MAC field including:

said ATM OUI identifier indicating that said incoming Ethernet frame comprises ATM traffic; and

a unique address of said E-Mux.

11. A method for transmitting information from an Ethernet network to an ATM network using an E-Mux performing the steps of:

establishing connection between an end station of said Ethernet network and an ATM switch of said ATM network based on a VPI/VCI destination address provided by said end station;

generating an outgoing Ethernet frame at said end station and transmitting same to said E-Mux;

extracting from said Ethernet outgoing frame a traffic type indicator, a frame payload and a source address;

generating an ATM adaptation layer 5 (AAL5) protocol data unit (PDU) from said frame payload and a traffic type indicator extracted from the type field of said outgoing frame; and

segmenting said PDU into a plurality of outgoing ATM cells and inserting a VPI/VCI destination address in the header of said cells from an address processor.

12. A method as claimed in claim 11, wherein said outgoing Ethernet frame comprises:

a destination MAC field including:

a unique ATM OUI identifier indicating that said outgoing Ethernet frame comprises ATM traffic; and

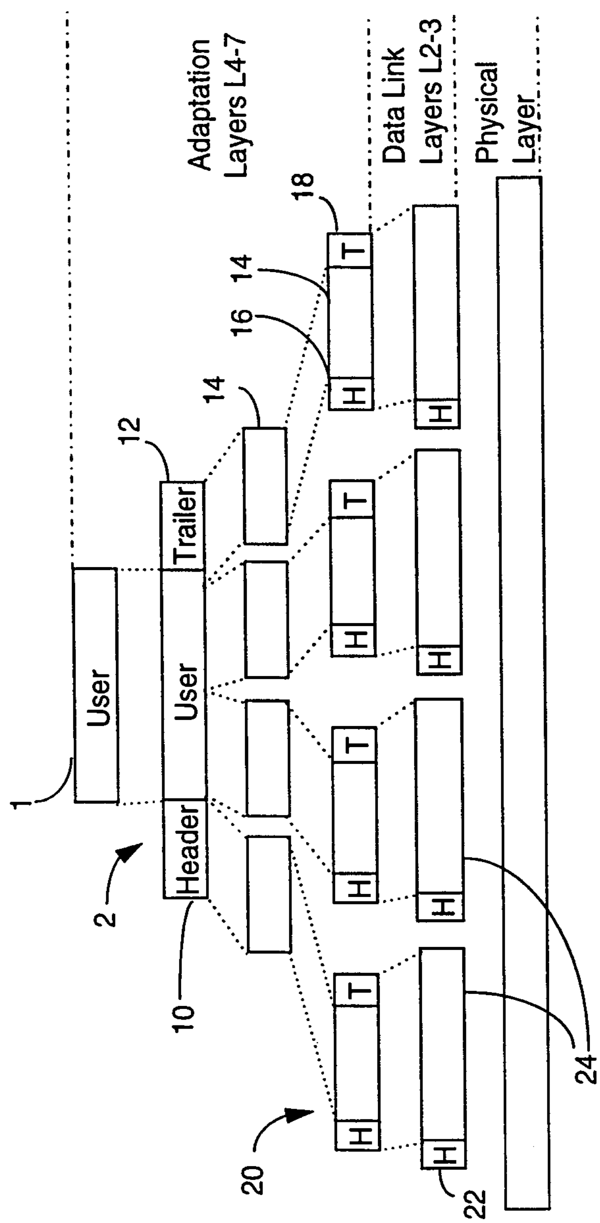
a unique address of said E-Mux;

a source MAC field including:

said ATM OUI identifier indicating that said outgoing Ethernet frame comprises ATM traffic; and

said VPI/VCI destination address specifying the address of said ATM cell.

FIGURE 1A
(Prior Art)



2/10

FIGURE 1B (Prior Art)

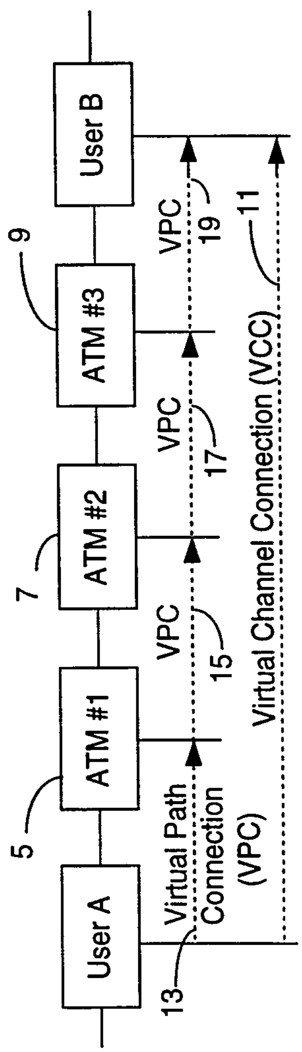


FIGURE 1C (Prior Art)

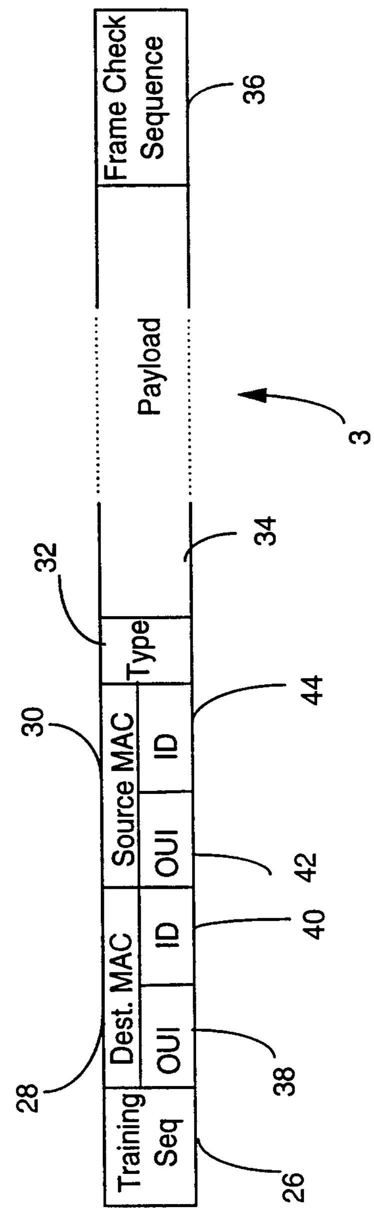


FIGURE 2

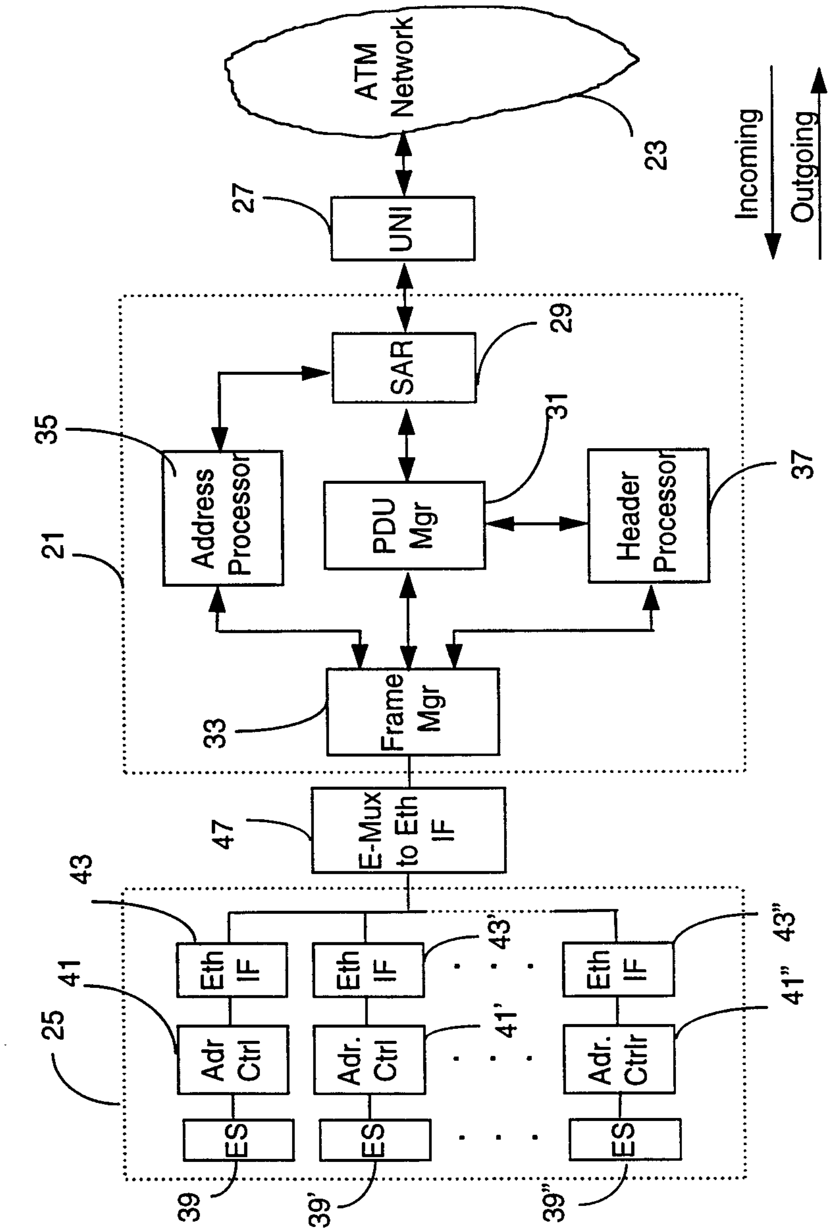

ATM Network
23
Incoming
Outgoing
UNI
27
SAR
29
Address Processor
35
PDU Mgr
31
Header Processor
37
21
Frame Mgr
33
E-Mux to Eth IF
47
43
Eth IF
43'
43"
Adr Ctrl
Adr. Ctrl
Adr. Ctrlr
41
41'
41"
25
ES
39
39'
39"

FIGURE 3A

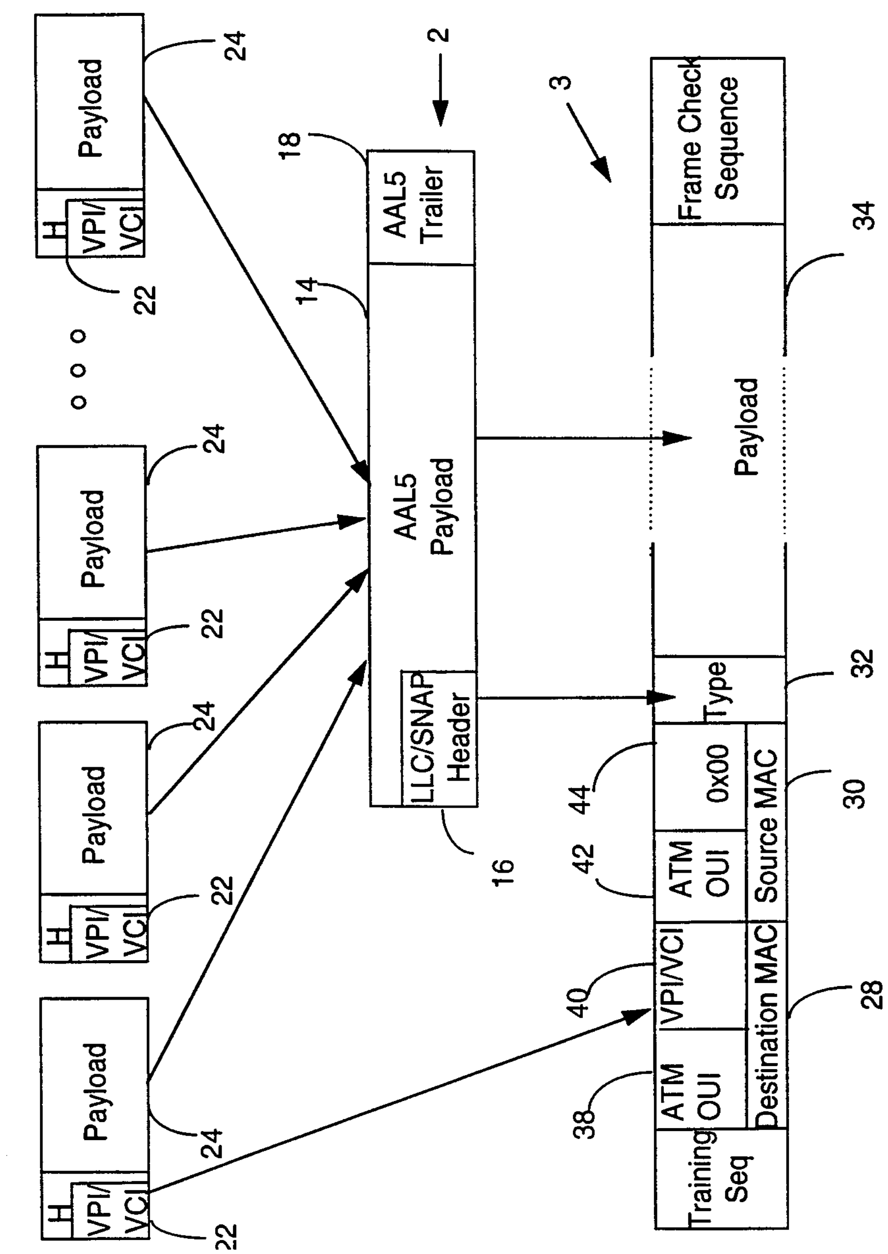
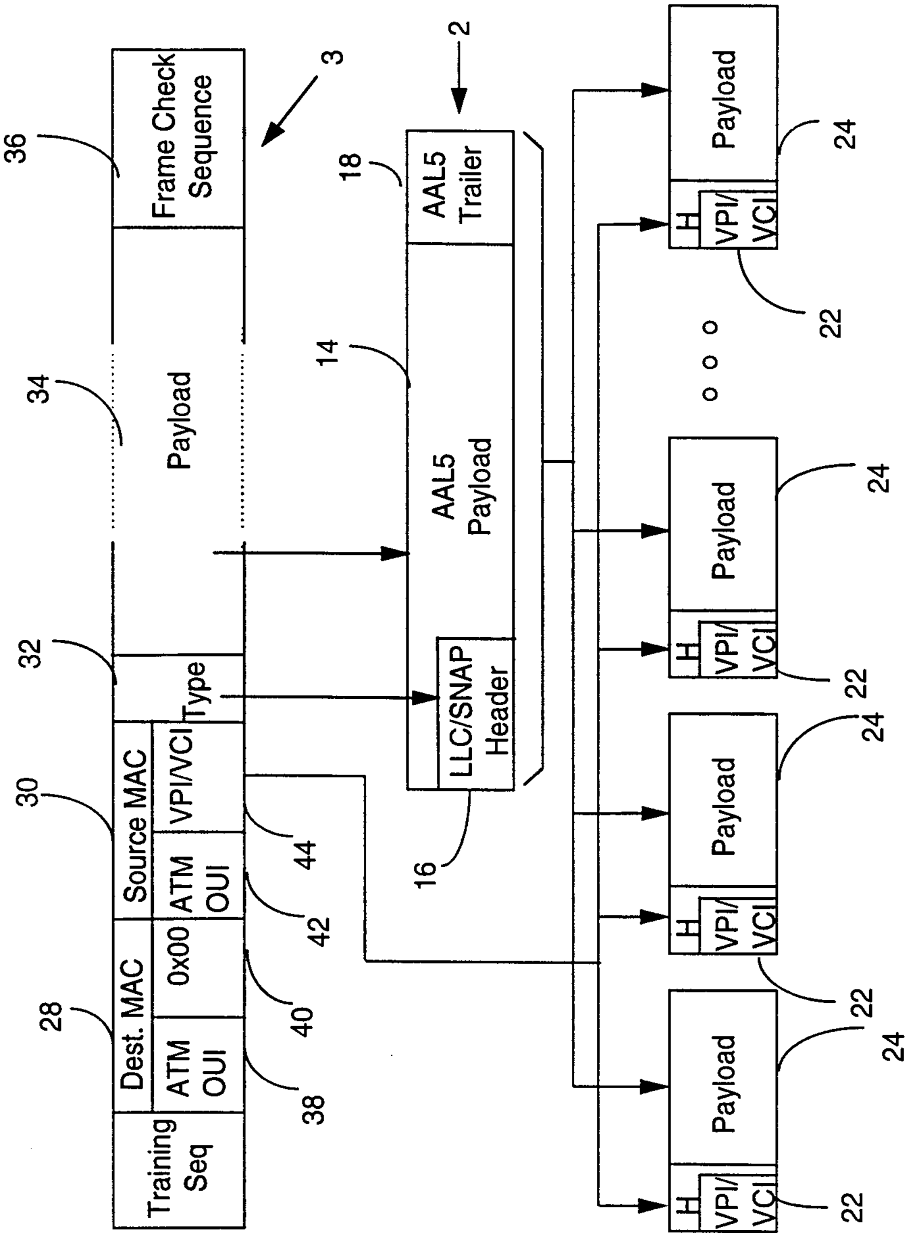
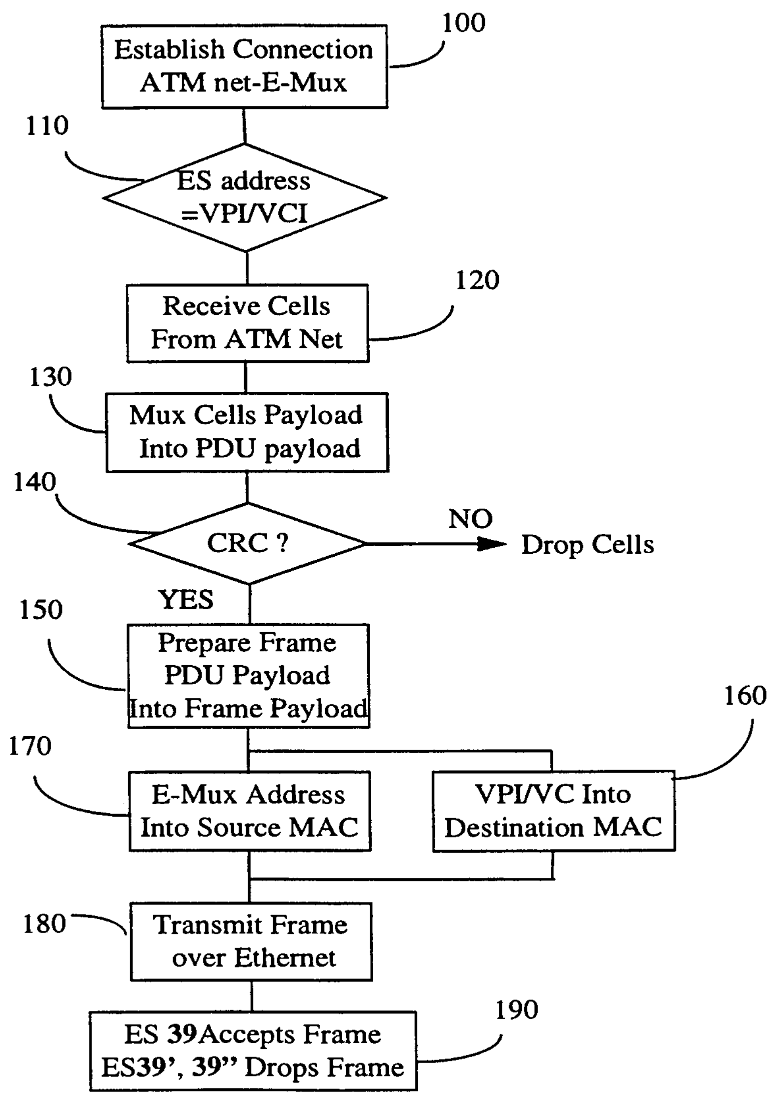

Payload
H
VPI/
VCI
22
24
AAL5
Trailer
18
14
AAL5
Payload
LLC/SNAP
Header
16
2
3
Frame Check
Sequence
34
Payload
Type
32
0x00
44
ATM
OUI
42
Source MAC
30
VPI/VCI
40
Destination MAC
28
ATM
OUI
38
Training
Seq

FIGURE 3B



Training Seq
Dest. MAC
ATM OUI
0x00
Source MAC
ATM OUI
VPI/VCI
Type
Payload
Frame Check Sequence
LLC/SNAP Header
AAL5 Payload
AAL5 Trailer
H
VPI/ VCI
Payload
2
3
14
16
18
22
24
28
30
32
34
36
38
40
42
44

FIGURE 4A



Establish Connection ATM net-E-Mux
100
110
ES address =VPI/VCI
Receive Cells From ATM Net
120
130
Mux Cells Payload Into PDU payload
140
CRC ?
NO
Drop Cells
YES
150
Prepare Frame PDU Payload Into Frame Payload
160
170
E-Mux Address Into Source MAC
VPI/VC Into Destination MAC
180
Transmit Frame over Ethernet
190
ES 39 Accepts Frame ES39', 39" Drops Frame

FIGURE 4B

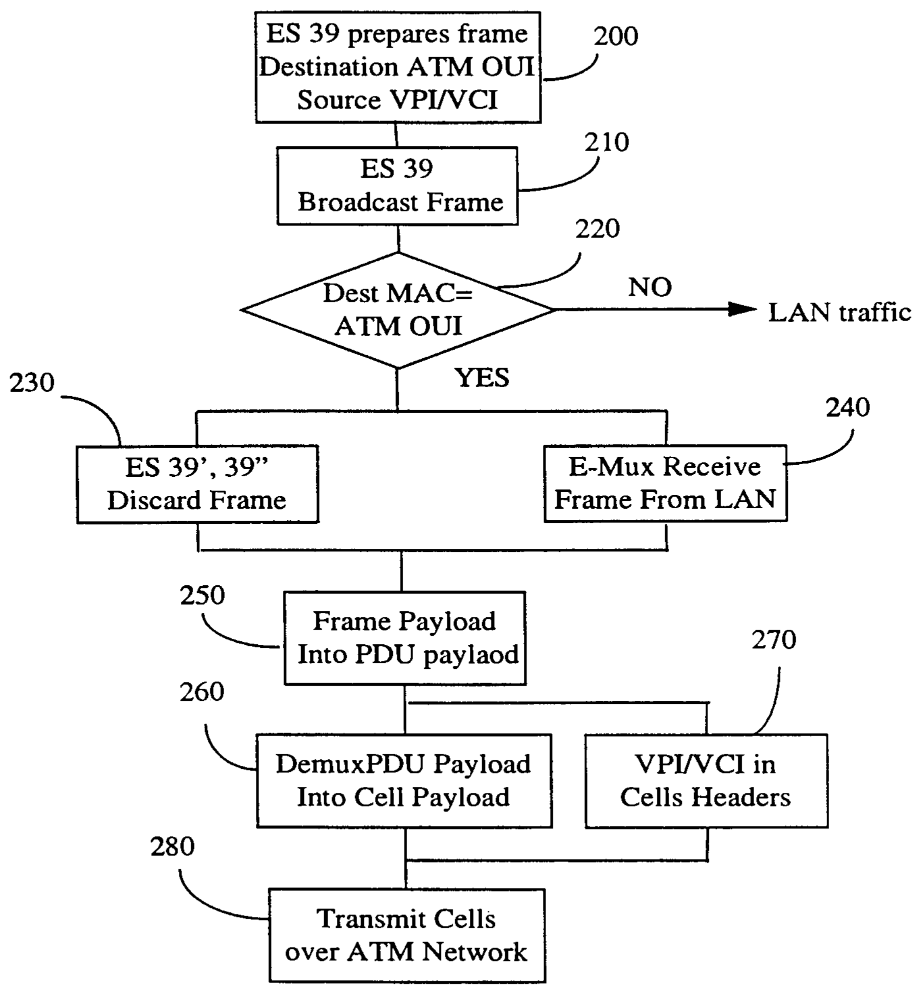

ES 39 prepares frame
Destination ATM OUI
Source VPI/VCI
200
ES 39
Broadcast Frame
210
220
Dest MAC=
ATM OUI
NO
LAN traffic
YES
230
ES 39', 39"
Discard Frame
240
E-Mux Receive
Frame From LAN
250
Frame Payload
Into PDU paylaod
270
260
DemuxPDU Payload
Into Cell Payload
VPI/VCI in
Cells Headers
280
Transmit Cells
over ATM Network

FIGURE 5

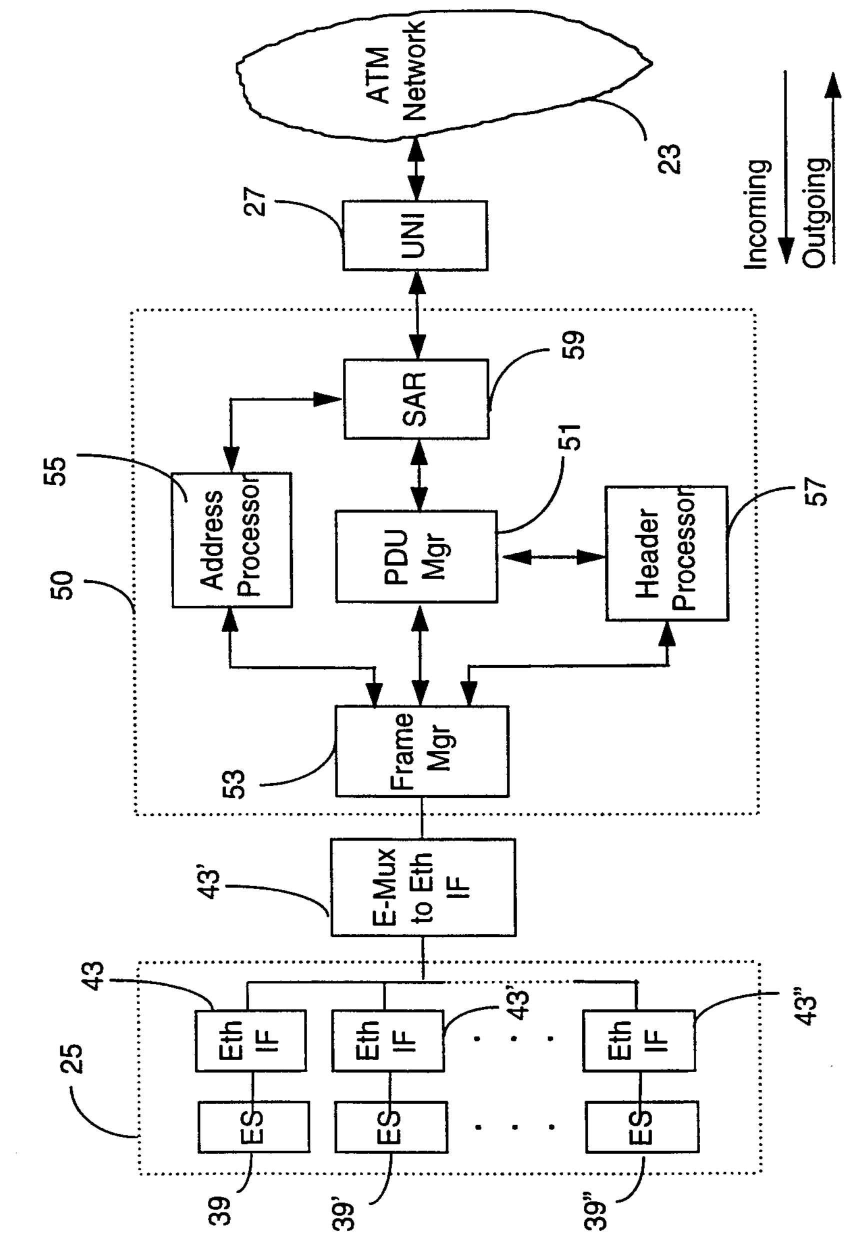

ATM Network
23
27
UNI
Incoming
Outgoing
59
SAR
55
Address Processor
51
PDU Mgr
57
Header Processor
50
53
Frame Mgr
43'
E-Mux to Eth IF
43
Eth IF
43'
43"
25
ES
39
39'
39"

FIGURE 6A

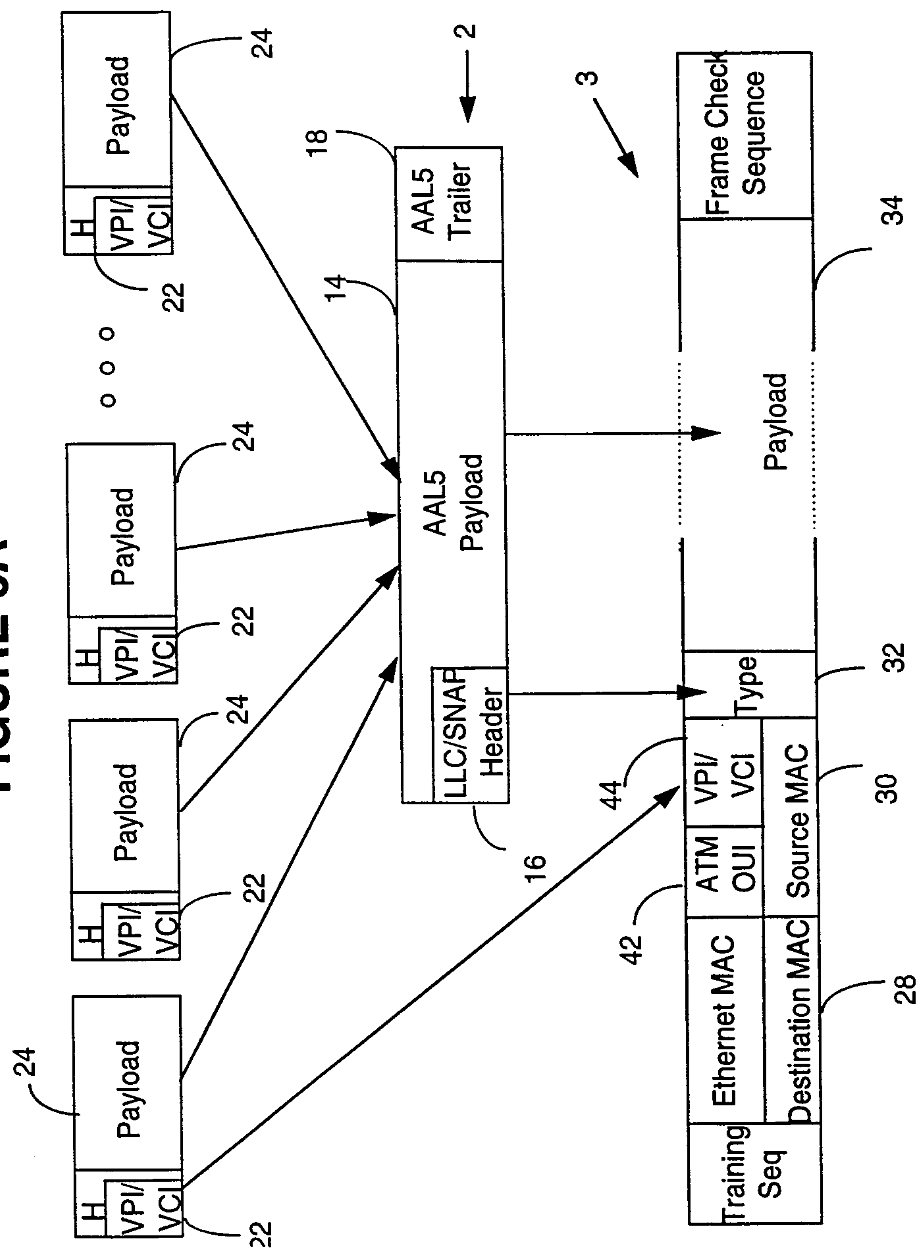
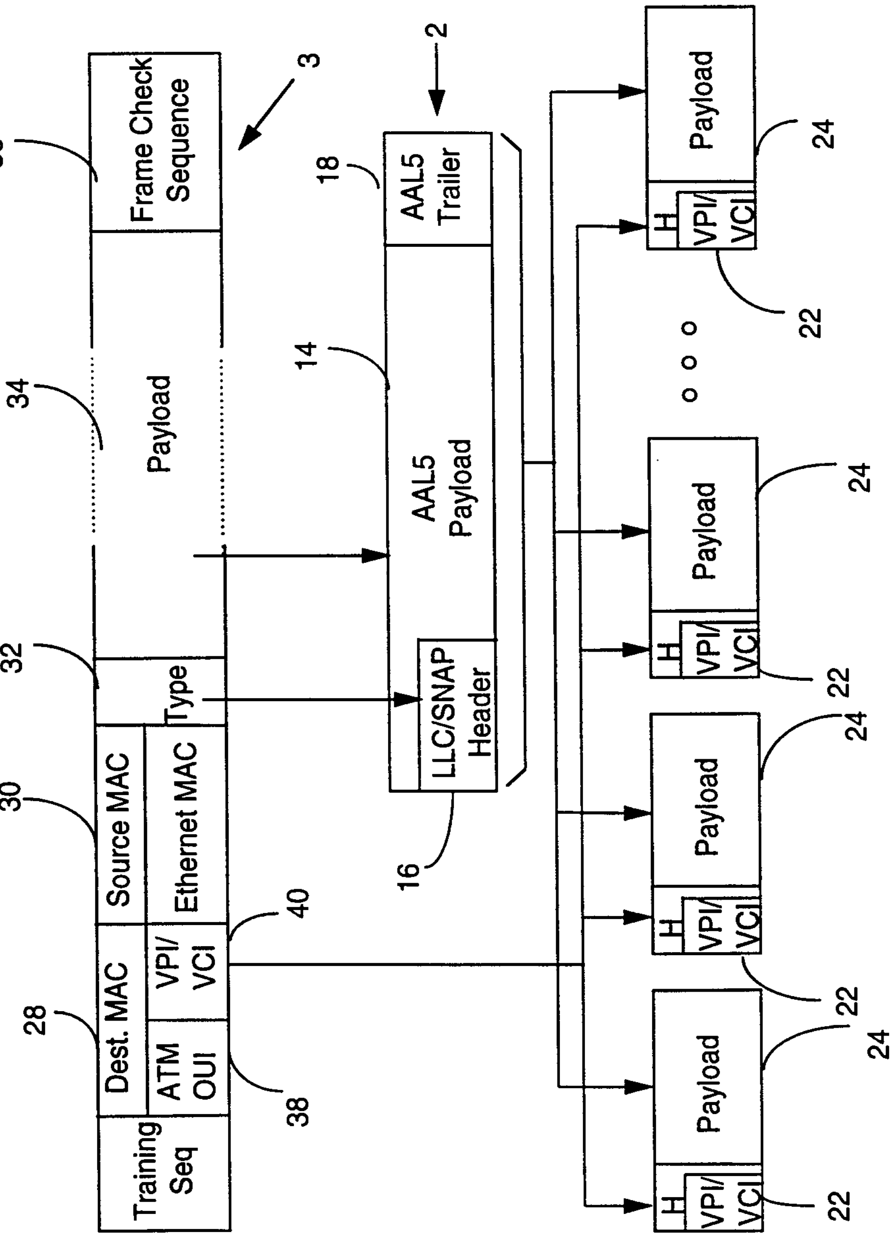

Payload
H
VPI/VCI
24
22
AAL5 Payload
AAL5 Trailer
LLC/SNAP Header
18
14
16
2
3
Frame Check Sequence
Payload
Type
34
32
VPI/VCI
ATM OUI
Ethernet MAC
Source MAC
Destination MAC
Training Seq
44
42
30
28

FIGURE 6B


Training Seq
Dest. MAC
ATM OUI
VPI/ VCI
Source MAC
Ethernet MAC
Type
Payload
Frame Check Sequence
LLC/SNAP Header
AAL5 Payload
AAL5 Trailer
H
VPI/ VCI
Payload
3
2
14
16
18
22
24
28
30
32
34
36
38
40

INTERNATIONAL SEARCH REPORT

Inte..ational Application No
PCT/CA 98/00197

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/66 H04Q11/04

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CASTRO R ET AL: "SUPPORT OF DATA COMMUNICATIONS IN AN ATM LAN" INFORMATION NETWORKS AND DATA COMMUNICATION, PROCEEDINGS OF THE IFIP TC6 INTERNATIONAL CONFERENCE ON INFORMATION NETWORKS AND DATA COMMUNICATION, FUNCHAL, MADEIRA ISLAND, PORTUGAL, APR. 18 - 21, 1994, no. CONF. 5, 18 April 1994, VEIGA P;DIPAK KHAKHAR (EDS), pages 277-295, XP000593298 see paragraph 2.3.4 ---	1-9,11

-/--

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 June 1998	26/06/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Staessen, B

2

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	SMITH J C: "10MBPS TO 155MBPS ATM USING THE IDT SARAMTM AS A CONCENTRATOR BROUTER CORE" WESCON '94. WESTERN ELECTRONIC SHOW AND CONVENTION, ANAHEIM, SEPT. 27 - 29, 1994, 27 September 1994, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, pages 495-502, XP000532615 paragraph "ATM Packet structuring" ---	1-12
A	MIRCHANDANI V ET AL: "AN INTERNETWORKING ARCHITECTURE FOR INTEGRATED VOICE AND DATA COMMUNICATIONS" PROCEEDINGS OF THE REGION 10 ANNUAL INTERNATIONAL CONFERENCE (TENCO, SINGAPORE, 22 - 26 AUG., 1994, vol. VOL. 2, no. CONF. 9, 22 August 1994, CHAN T K Y (ED), pages 749-753, XP000528218 see paragraph 3 ---	1-12
A	CAMARDA P ET AL: "A ROUTER FOR THE INTERCONNCETION OF ETHERNET LOCAL AREA NETWORKS VIA AN ATM NETWORK" PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON INTEGRATED BROADBAND SERVICES AND NETWORKS, LONDON, 15 - 18 OCT., 1990, no. -, 15 October 1990, INSTITUTION OF ELECTRICAL ENGINEERS, pages 283-288, XP000410619 paragraph "Router Description"; ---	1-12
A	PAONE R ET AL: "FEASIBILITY MODEL OF A FLEXIBLE BUSINESS CUSTOMER PREMISES NETWORK" ELECTRONICS AND COMMUNICATION ENGINEERING JOURNAL, vol. 4, no. 4, 1 August 1992, pages 215-224, XP000307899 see page 222 see page 223 -----	1-12

2

Electronic Acknowledgement Receipt

EFS ID:	9762021
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Hasan M. Rashid/Melissa Molchan
Filer Authorized By:	Hasan M. Rashid
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN
Receipt Date:	29-MAR-2011
Filing Date:	16-AUG-2007
Time Stamp:	13:49:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	0066IDS.pdf	125965 1e49f81f0da67d59ba4a028047e60183012a066c	no	2

Warnings:

Information:

This is not an USPTO supplied IDS fillable form

2	Foreign Reference	WO9843396.pdf	1348054 02fb89aa88c9d669c72e526b2d6b8ded86400824	no	37

Warnings:

Information:

3	NPL Documents	101EPSearchReport.pdf	316610 3c556bd662e25af934512ea23fc10a393885c6e0	no	7

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

4	NPL Documents	105EPSearchReport.pdf	216885 f55eea81ea84e25bf6755cf8572244c2c2a61312	no	6

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

5	NPL Documents	2NOA0057.pdf	2721824 f8e309ce9dee16e42daecb0b92faae39880f762a	no	34

Warnings:

Information:

6	NPL Documents	Hollenbeck.pdf	2638150 c8d6d8db4c54893bb4e2b3e2e62315fb1adb77b5	no	34

Warnings:

Information:

7	NPL Documents	Tannenbaum.pdf	853980 aef4faaf476d56146d79ce1cc0a775fb29459767	no	18

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

Total Files Size (in bytes):	8221468

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

23630 7590 04/04/2011

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
LIM, KRISNA	
ART UNIT	PAPER NUMBER
2453	

DATE MAILED: 04/04/2011

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/839,987	08/16/2007	Victor Larson	77580-0066 (VRNK-1CP2DVCN	9470

TITLE OF INVENTION: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$300	$0	$1810	07/05/2011

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23630 7590 04/04/2011

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/839,987	08/16/2007	Victor Larson	77580-0066 (VRNK-1CP2DVCN	9470

TITLE OF INVENTION: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$300	$0	$1810	07/05/2011

EXAMINER	ART UNIT	CLASS-SUBCLASS
LIM, KRISNA	2453	709-227000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
   - ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
   - ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
   (1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
   (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
   1 ____________________
   2 ____________________
   3 ____________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies ____________________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number ____________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature ______________________________ Date ______________________________

Typed or printed name ______________________________ Registration No. ______________________________

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/839,987	08/16/2007	Victor Larson	77580-0066 (VRNK-1CP2DVCN	9470

23630 7590 04/04/2011

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER
LIM, KRISNA

ART UNIT	PAPER NUMBER
2453	

DATE MAILED: 04/04/2011

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 15 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 15 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 11/839,987	Applicant(s) LARSON ET AL.	
	Examiner Krisna Lim	Art Unit 2453	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the communication filed 01/10/2011*.

2. ☒ The allowed claim(s) is/are *1-18*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)
1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Krisna Lim/
Primary Examiner, Art Unit 2453

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11839987	LARSON ET AL.
	Examiner	**Art Unit**
	Krisna Lim	2453

SEARCHED

Class	Subclass	Date	Examiner
709	225-229, 245	2/13/2010	kl
726	15	2/13/2010	kl
709	225-229, 245	3/25/2011	kl
726	15	3/25/2011	kl

SEARCH NOTES

Search Notes	Date	Examiner
EAST, Inventors	2/13/2010	kl

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
709	227, 228	2/13/2010	kl
709	227, 228	3/25/2011	kl

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08/16/2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0066**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1019	5,870,610	02/1999	Beyda et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 -Number 4 -Kind Code5 *(if known)*	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	B1003	EP0838930	4/29/1988	Digital Equipment Corporation			
	B1004	EP0814589	12/29/1997	AT&T Corp.			
	B1005	GB2317792	04/01/1998	Secure Computing Corporation			
	B1006	WO98/27783	06/25/1998	Northern Telecom Limited			
	B1007	WO99/11019	03/04/1999	V One Corp			
	B1008	GB2334181	08/11/1999	NEC Technologies			
	B1009	GB2340702	02/23/2000	Sun Microsystems Inc.			

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1244	Baumgartner et al, “Differentiated Services: A New Approach for Quality of Service in the Internet,” International Conference on High Performance Networking, 255-273 (1998)	
	C1245	Chapman et al., “Domain Name System (DNS),” 278-296 (1995)	
	C1246	Davila et al., “Implementation of Virtual Private Networks at the Transport Layer,” M. Mambo, Y. Zheng (Eds), Information Security (Second International) Workshop, ISW’ 99. Lecture Notes in Computer Science (LNCS), Vol. 1729; 85-102 (1999)	
	C1247	De Raadt et al., “Cryptography in OpenBSD,” 10 pages (1999)	
	C1248	Eastlake, “Domain Name System Security Extensions,” Internet Citation, Retrieved from the Internet: URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-dnssec-secext2-05.txt (1998)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08/16/2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0066**

	C1249	Gunter et al., "An Architecture for Managing QoS-Enabled VRNs Over the Internet," Proceedings 24th Conference on Local Computer Networks. LCN' 99 IEEE Comput. Soc Los Alamitos, CA, pages 122-131 (1999)	
	C1250	Shimizu, "Special Feature: Mastering the Internet with Windows 2000", Internet Magazine, 63:296-307 (2000)	
	C1251	Stallings, "Cryptography and Network Security," Principals and Practice, 2nd Edition, pages 399-440 (1999)	
	C1252	Takata, "U.S. Vendors Take Serious Action to Act Against Crackers – A Tracking Tool and a Highly Safe DNS Software are Released", Nikkei Communications, 257:87(1997)	
	C1253	Wells, Email (Lancasterb1be@mail.msn.com), Subject: "Security Icon," (1998)	

/Krisna Lim/ 03/25/2011

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1021	4,920,484	04-24-1990	Ranade	
	A1022	4,933,846	06-12-1990	Humphrey et al.	
	A1023	4,988,990	01-29-1991	Warrior	
	A1024	5,164,988	11-17-1992	Matyas	
	A1025	5,276,735	01-04-1994	Boebert et al.	
	A1026	5,329,521	07-12-1994	Walsh et al.	
	A1027	5,341,426	08-23-1994	Barney et al.	
	A1028	5,367,643	11-22-1994	Chang et al.	
	A1029	5,559,883	09-24-1996	Williams	
	A1030	5,561,669	10-01-1996	Lenney et al.	
	A1031	5,588,060	12-24-1996	Aziz	
	A1032	5,625,626	04-29-1997	Umekita	
	A1033	5,654,695	08-05-1997	Olnowich et al.	
	A1034	5,682,480	10-28-1997	Nakagawa	
	A1035	5,689,566	11/18/1997	Nguyen	
	A1036	5,740,375	04-14-1998	Dunne et al.	
	A1037	5,774,660	06-30-1998	Brendel et al.	
	A1038	5,787,172	07-28-1998	Arnold	
	A1039	5,790,548	08-04-1998	Sitaraman et al.	
	A1040	5,796,942	08-18-1998	Esbensen	
	A1041	5,805,801	09-08-1998	Holloway et al.	
	A1042	5,842,040	11-24-1998	Hughes et al.	
	A1043	5,845,091	12-01-1998	Dunne et al.	
	A1044	5,867,650	02-02-1998	Osterman	
	A1045	5,878,231	05-02-1999	Baehr et al.	
	A1046	5,892,903	04-06-1999	Klaus	
	A1047	5,905,859	05-18-1999	Holloway et al.	
	A1048	5,918,018	06/29/1999	Gooderum et al.	
	A1049	5,918,019	06-29-1999	Valencia	
	A1050	5,996,016	11-30-1999	Thalheimer et al.	
	A1051	6,006,259	12-21-1999	Adelman et al.	
	A1052	6,006,272	12-21-1999	Aravamudan et al.	
	A1053	6,016,318	01-18-2000	Tomoike	
	A1054	6,016,512	01-18-2000	Huitema	
	A1055	6,041,342	03-21-2000	Yamaguchi	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

	A1056		6,061,736	05-09-2000	Rochberger et al.	
	A1057		6,092,200	07-18-2000	Muniyappa et al.	
	A1058		6,119,234	09-12-2000	Aziz et al.	
	A1059		6,147,976	11-14-2000	Shand et al.	
	A1060		6,157,957	12-05-2000	Berthaud	
	A1061		6,158,011	12-05-2000	Chen et al.	
	A1062		6,168,409	01-02-2001	Fare	
	A1063		6,175,867	01-16-2001	Taghadoss	
	A1064		6,178,409	01-23-2001	Weber et al.	
	A1065		6,178,505	01-23-2001	Schneider et al.	
	A1066		6,179,102	01-30-2001	Weber et al.	
	A1067		6,222,842	04-24-2001	Sasyan et al.	
	A1068		6,233,618	05-15-2001	Shannon	
	A1069		6,243,360	06-05-2001	Basilico	
	A1070		6,243,749	06-05-2001	Sitaraman et al.	
	A1071		6,243,754	06-05-2001	Guerin et al.	
	A1072		6,256,671	07-03-2001	Strentzsch et al.	
	A1073		6,263,445	07-17-2001	Blumenau	
	A1074		6,286,047	09-04-2001	Ramanathan et al.	
	A1075		6,301,223	10-09-2001	Hrastar et al.	
	A1076		6,308,213	10/23/2001	Valencia	
	A1077		6,308,274	10-23-2001	Swift	
	A1078		6,311,207	10-30-2001	Mighdoll et al.	
	A1079		6,324,161	11-27-2001	Kirch	
	A1080		6,330,562	12-11-2001	Boden et al.	
	A1081		6,332,158	12-18-2001	Risley et al.	
	A1082		6,353,614	03-05-2002	Borella et al.	
	A1083		6,425,003	07-23-2002	Herzog et al.	
	A1084		6,430,155	08-06-2002	Davie et al.	
	A1085		6,430,610	08-06-2002	Carter	
	A1086		6,487,598	11-26-2002	Valencia	
	A1087		6,505,232	01-07-2003	Mighdoll et al.	
	A1088		6,510,154	01-21-2003	Mayes et al.	
	A1089		6,549,516	04-15-2003	Albert et al.	
	A1090		6,571,296	05-27-2002	Dillon	
	A1091		6,571,338	05-27-2003	Shaio et al.	
	A1092		6,581,166	07-17-2003	Hirst et al.	
	A1093		6,606,708	08-12-2003	Devine et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

	A1094	6,618,761	09-09-2003	Munger et al.	
	A1095	6,671,702	12-30-2003	Kruglikov et al.	
	A1096	6,687,551	02-03-2004	Steindl	
	A1097	6,714,970	03-30-2004	Fiveash et al.	
	A1098	6,717,949	04-06-2004	Boden et al.	
	A1099	6,751,738	06-15-2004	Wesinger, Jr. et al.	
	A1100	6,760,766	07-06-2004	Sahlqvist	
	A1101	6,826,616	11-30-2004	Larson et al.	
	A1102	6,839,759	01-04-2005	Larson et al.	
	A1103	7,010,604	03-07-2006	Munger et al.	
	A1104	7,133,930	11-07-2006	Munger et al.	
	A1105	7,188,180	03-06-2007	Larson et al.	
	A1106	7,197,563	03-27-2007	Sheymov et al.	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B1	US2002/0004898	01-10-2002	Droge	
	B2	US2003/0196122	10-16-2003	Wesinger, Jr., et al.	
	B3	US2005/0055306	03-10-2005	Miller et al.	
	B4	US2006/0059337	03-16-2006	Polyhonen et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 -Number 4 -Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	C1010	DE19924575	12-02-1999	Provino et al.			
	C1011	EP0858189	08-12-1998	Maciel et al.			
	C1012	EP836306	04-15-1998	Hewlett Packard Co.			
	C1013	WO0150688	07-12-2001	Kriens			
	C1014	WO9855930	12-10-1998	Tang			
	C1015	WO9859470	12-30-1998	Kanter et al.			
	C1016	WO9938081	07-29-1999	Paulsen et al.			
	C1017	WO9948303	09-23-1999	Cox et al.			

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1254	Alan 0. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/ draft302.txt on Feb. 4, 2002, 56 pages.	
	D1255	August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.	
	D1256	D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-375.	
	D1257	D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.	
	D1258	Davila J et al, "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Work-shop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-666.	
	D1259	Deposition Transcript for Gary Tomlinson dated February 27, 2009.	
	D1260	Dolev, Shlomi and Ostrovsky, Rafil, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.	
	D1261	Donald E. Eastlake, 3rd, "Domain Name System Security Extensions", INTERNET DRAFT, Apr. 1998, pp. 1-51.	
	D1262	F. Halsall, "Data Communications, Computer Networks and Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.	
	D1263	Final Office Action dated April 11,2005 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016).	
	D1264	Final Office Action dated April 8, 2010 from corresponding US Application Number 11/679,416 (Our Ref. No.077580-0015).	
	D1265	Final Office Action dated December 7, 2005 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037).	
	D1266	Final Office Action dated February 11, 2004 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016).	
	D1267	Final Office Action dated February 9, 2010 from corresponding US Application Number 11/301,022 (Our Ref. No.077580-0044).	
	D1268	Final Office Action dated October 21, 2010 from corresponding US Application Number 11/840,560 (Our Ref. No.077580-0063).	
	D1269	Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/ doc/glossary.html on Feb. 21, 2002, 25 pages.	
	D1270	J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan _trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

	D1271	James E. Bellaire, "New Statement of Rules-Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page. (Due to difficulty finding a hard copy of this reference, a copy of this reference is not included herewith. This reference, however was first submitted to the Patent Office in an IDS in application No. 11/679,416 on 11/13/2007 as ref. No. C12. The office is requested to see this reference at that location).	
	D1272	Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.	
	D1273	Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606, 1 page.	
	D1274	Linux FreeS/WAN Index File, printed from http://liberty.freewan.org/freeswan_trees/freeswan-1.3/doc/ on Feb. 21, 2002, 3 Pages. (Due to difficulty finding a hard copy of this reference, a copy of this reference is not included herewith. This reference, however was first submitted to the Patent Office in an IDS in application No. 11/679,416 on 11/13/2007 as ref. No. C15. The office is requested to see this reference at that location).	
	D1275	Non-Final Office Action dated December 14, 2010 from corresponding US Application Number 11/839,937 (Our Ref. No. 077580-0064)	
	D1276	Non-Final Office Action dated December 7, 2010 from corresponding US Application Number 11/679,416 (Our Ref. No. 077580-0015)	
	D1277	Notice of Allowance dated January 11, 2008 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D1278	Non-Final Office Action dated July 1, 2010 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065).	
	D1279	Non-Final Office Action dated July 14, 2010 from corresponding US Application Number 11/840,508 (Our Ref. No.077580-0057).	
	D1280	Non-Final Office Action dated June 15, 2007 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D1281	Non-Final Office Action dated June 16, 2003 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016).	
	D1282	Non-Final Office Action dated June 24, 2004 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D1283	Non-Final Office Action dated June 3, 2005 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037.	
	D1284	Non-Final Office Action dated June 7, 2010 from corresponding US Application Number 11/924,460 (Our Ref. No.077580-0073).	
	D1285	Non-Final Office Action dated June 8, 2009 from corresponding US Application Number 11/679,416 (Our Ref. No.077580-0015).	
	D1286	Non-Final Office Action dated June 9, 2010 from corresponding US Application Number 11/924,460 (Our Ref. No.077580-0073).	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

	D1287	Non-Final Office Action dated March 1, 2004 from corresponding US Application Number 10/401,888 (Our Ref. No. 077580-0038)	
	D1288	Non-Final Office Action dated March 19, 2010 from corresponding US Application Number 11/840,560 (Our Ref. No.077580-0063).	
	D1289	Non-Final Office Action dated March 21, 2007 from corresponding US Application Number 10/714,849 (Our Ref. No. 077580-0042)	
	D1290	Non-Final Office Action dated March 28, 2006 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D1291	Non-Final Office Action dated March 5, 2009 from corresponding US Application Number 11/301,022 (Our Ref. No.077580-0044).	
	D1292	Non-Final Office Action dated May 19, 2006 from corresponding US Application Number 10/702,486 (Our Ref. No.077580-0039).	
	D1293	Non-Final Office Action dated May 4, 2004 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016).	
	D1294	Non-Final Office Action dated October 18, 2005 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D1295	Non-Final Office Action dated October 21, 2004 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037).	
	D1296	Non-Final Office Action dated October 30, 2006 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D1297	Non-Final Office Action dated September 17, 2008 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065).	
	D1298	Non-Final Office Action dated September 2, 2009 from corresponding US Application Number 11/924,460 (Our Ref. No.077580-0073).	
	D1299	Notice of Allowance dated April 18, 2006 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D1300	Notice of Allowance dated April 3, 2009 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	
	D1301	Notice of Allowance dated April 5, 2006 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D1302	Notice of Allowance dated August 10, 2005 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016)	
	D1303	Notice of Allowance dated August 16, 2004 from corresponding US Application Number 10/702,580 (Our Ref. No. 077580-0041)	
	D1304	Notice of Allowance dated August 17, 2004 from corresponding US Application Number 10/702,522 (Our Ref. No. 077580-0040)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

	D1305	Notice of Allowance dated December 5, 2005 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016)	
	D1306	Notice of Allowance dated February 16, 2006 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D1307	Notice of Allowance dated January 13, 2010 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	
	D1308	Notice of Allowance dated January 28, 2010 from corresponding US Application Number 11/840,508 (Our Ref. No.077580-0057)	
	D1309	Notice of Allowance dated January 4, 2011 from corresponding US Application Number 11/301,022 (Our Ref. No. 077580-0044)	
	D1310	Notice of Allowance dated July 1, 2008 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D1311	Notice of Allowance dated July 21, 2004 from corresponding US Application Number 10/401,888 (Our Ref. No. 077580-0038)	
	D1312	Notice of Allowance dated March 17, 2006 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D1313	Notice of Allowance dated May 27, 2009 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	
	D1314	Notice of Allowance dated May 9, 2006 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D1315	Notice of Allowance dated November 19, 2009 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	
	D1316	Notice of Allowance dated November 21, 2006 from corresponding US Application Number 10/702,486 (Our Ref. No.077580-0039)	
	D1317	Notice of Allowance dated October 29, 2007 from corresponding US Application Number 10/714,849 (Our Ref. No. 077580-0042)	
	D1318	Notice of Allowance dated September 16, 2009 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	
	D1319	P. Srisuresh et al., "DNS extensions to Network address Translators (DNS_ALG)", Internet Draft, Jul. 1998, pp. 1-27.	
	D1320	PCT International Search Report for related PCT Application No.: PCT/US01/13261, 8 pages (Our Ref. No. 077580-0032).	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

	D1321	PCT International Search Report for related PCT Application No.: PCT/US99/25323, 3 pages (Our Ref. No. 077580-0062).	
	D1322	PCT International Search Report for related PCT Application No.: PCT/US99/25325, 3 pages (Our Ref. No. 077580-0061).	
	D1323	Reiter, Michael K. and Rubin, Aviel D. (AT&T Labs-Research), "Crowds: Anonymity for Web Transactions", pp. 1-23.	
	D1324	RFC 2401 (dated Nov. 1998) Security Architecture for the Internet Protocol (RTP).	
	D1325	RFC 2543-SIP (dated March 1999): Session Initiation Protocol (SIP or SIPS).	
	D1326	Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages. (Due to difficulty finding a hard copy of this reference, a copy of this reference is not included herewith. This reference, however was first submitted to the Patent Office in an IDS in application No. 11/679,416 on 11/13/2007 as ref. No. C20. The office is requested to see this reference at that location).	
	D1327	Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.	
	D1328	Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.	
	D1329	Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.	
	D1330	Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.	
	D1331	Search Report, IPER (dated Jan. 14, 2003), International Application No. PCT/US01/13260.	
	D1332	Search Report, IPER (dated Nov. 13, 2002), International Application No. PCT/US01/04340.	
	D1333	Shankar, A.U. "A verified sliding window protocol with variable flow control". Proceedings of ACM SIGCOMM conferece on Communications architectures & protocols. pp. 84-91, ACM Press, NY,NY 1986.	
	D1334	Shree Murthy et al., "Congestion-Oriented Shortest Multi-path Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.	
	D1335	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 9:00 AM.	
	D1336	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 1:00 PM.	
	D1337	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 9:00 AM.	
	D1338	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 1:30 PM.	
	D1339	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 9:00 AM.	
	D1340	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 1:15 PM.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

	D1341	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 9:00 AM.	
	D1342	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 12:35 PM.	
	D1343	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 8:45 AM.	
	D1344	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 1:30 PM.	
	D1345	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 9:00 AM.	
	D1346	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 1:30 PM.	
	D1347	W. Stallings, "Cryptography And Network Security", 2nd, Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	03/25/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[X] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Toby H. Kusmer

Date: 2/9/11

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 27365439-1.077580.0066

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Index of Claims	**Application/Control No.** 11839987	**Applicant(s)/Patent Under Reexamination** LARSON ET AL.
	Examiner Krisna Lim	**Art Unit** 2453

✓	**Rejected**	**-**	**Cancelled**	**N**	**Non-Elected**	**A**	**Appeal**
=	**Allowed**	**÷**	**Restricted**	**I**	**Interference**	**O**	**Objected**

☒ **Claims renumbered in the same order as presented by applicant** ☐ **CPA** ☒ **T.D.** ☐ **R.1.47**

CLAIM		DATE								
Final	Original	06/05/2009	12/29/2009	02/13/2010	07/04/2010	03/25/2011				
	1	✓	✓	=	✓	=				
	2		O	=	✓	=				
	3		O	=	✓	=				
	4		O	=	✓	=				
	5		O	=	✓	=				
	6		O	=	✓	=				
	7		O	=	✓	=				
	8		O	=	✓	=				
	9		O	=	✓	=				
	10		O	=	✓	=				
	11		O	=	✓	=				
	12		O	=	✓	=				
	13		O	=	✓	=				
	14		O	=	✓	=				
	15		O	=	✓	=				
	16		O	=	✓	=				
	17		O	=	✓	=				
	18		O	=	✓	=				

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11839987	LARSON ET AL.
	Examiner	**Art Unit**
	Krisna Lim	2453

ORIGINAL		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
709	227	G	0	6	F	15 / 173 (2006.01.01)						

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
709	228				

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☒ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	18	
/Krisna Lim/ Primary Examiner.Art Unit 2453	3/25/2011	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	27

.Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number.	**077580-0066**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
KL	A1044	5,590,285	12/31/19996	Krause et al.	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number 4-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
KL	C9	WO9843396	10/01/1998	Northern Telecom Limited			

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
KL	D81	European Search Report dated January 24, 2011 from corresponding European Application Number 10011949.4	
KL	D82	European Search Report dated March 17, 2011 from corresponding European Application Number 10184502.2	
KL	D83	Hollenbeck et al., "Registry Registrar Protocol (RRP) Version 1.1.0; Internet Engineering Task Force, 34 pages (1999)	
KL	D84	Notice of Allowance dated March 14, 2011 from corresponding US Application Number 11/840,508 (Our Ref. No.077580-0057)	
KL	D85	Tannenbaum, "Computer Networks," pages 202-219 (1996)	

KRISNA LIM
PRIMARY EXAMINER

4/14/2011

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/839,987	08/16/2007	Victor Larson	77580-0066 (VRNK-1CP2DVCN	9470

23630 7590 04/20/2011
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
LIM, KRISNA	
ART UNIT	**PAPER NUMBER**
2453	
NOTIFICATION DATE	**DELIVERY MODE**
04/20/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mweipdocket@mwe.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
11839987	8/16/07	LARSON ET AL.	77580-0066 (VRNK-1CP2DVCN

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
Krisna Lim	
ART UNIT	**PAPER**
2453	20110414

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

Attached herewith is a copy of IDS filed 03/29/2011 with Examiner's initial and dated.

/Krisna Lim/
Primary Examiner, Art Unit 2453

PTO-90C (Rev.04-03)

.Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/839,987**
	Filing Date	**08-16-2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0066**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1044	5,590,285	12/31/19996	Krause et al.	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 -Number 4 -Kind Code5 *(if known)*	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	C9	WO9843396	10/01/1998	Northern Telecom Limited			

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D81	European Search Report dated January 24, 2011 from corresponding European Application Number 10011949.4	
	D82	European Search Report dated March 17, 2011 from corresponding European Application Number 10184502.2	
	D83	Hollenbeck et al., “Registry Registrar Protocol (RRP) Version 1.1.0; Internet Engineering Task Force, 34 pages (1999)	
	D84	Notice of Allowance dated March 14, 2011 from corresponding US Application Number 11/840,508 (Our Ref. No.077580-0057)	
	D85	Tannenbaum, “Computer Networks,” pages 202-219 (1996)	

/Krisna Lim/ 04/14/2011

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23630 7590 06/06/2011

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/839,987	08/16/2007	Victor Larson	77580-0066 (VRNK-1CP3DVCN)	9470

TITLE OF INVENTION: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$300	$0	$1810	07/05/2011

EXAMINER	ART UNIT	CLASS-SUBCLASS
LIM, KRISNA	2453	709-227000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 ______
2 McDermott Will & Emery LLP
3 ______

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: VIRNETX, INCORPORATED

(B) RESIDENCE: (CITY and STATE OR COUNTRY): SCOTTS VALLEY, CA

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☑ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☑ Issue Fee
☑ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies ______

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 501133 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /Toby H. Kusmer/ Date June 17, 2011

Typed or printed name Toby H. Kusmer Registration No. 26,418

Electronic Patent Application Fee Transmittal

Application Number:	11839987
Filing Date:	16-Aug-2007
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer./Mary Fontinha
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	1501	1	1510	1510
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1810**

Electronic Acknowledgement Receipt

EFS ID:	10334007
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Mary Fontinha
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN
Receipt Date:	17-JUN-2011
Filing Date:	16-AUG-2007
Time Stamp:	17:15:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1810
RAM confirmation Number	4199
Deposit Account	501133
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	PTOL85.pdf	299977 f8bc9a8e357ac136ed10c4a595c4eb79495222d5	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32364 1174f5991b61c0bfa9a358ab9b9601128a4c23a7	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	332341	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/839,987	07/26/2011	7987274	77580-0066 (VRNK-1CP2DVCN	9470

23630 7590 07/06/2011

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 15 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Victor Larson, Fairfax, VA;
Robert Dunham Short III, Leesburg, VA;
Edmund Colby Munger, Crownsville, MD;
Michael Williamson, South Riding, VA;

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/839,987	07/26/2011	7987274	77580-0066	9470

(VRNK-1CP2DVCN

23630 7590 07/06/2011

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 15 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Victor Larson, Fairfax, VA;
Robert Dunham Short III, Leesburg, VA;
Edmund Colby Munger, Crownsville, MD;
Michael Williamson, South Riding, VA;

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas Tyler Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 6:13-cv-00351	DATE FILED 4/22/2013	U.S. DISTRICT COURT Eastern District of Texas Tyler Division
PLAINTIFF VirnetX Inc. and Science Applications International Corporation		DEFENDANT Microsoft Corporation

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,502,135	12/31/2002	VirnetX Inc.
2 7,188,180	3/6/2007	VirnetX Inc.
3 7,418,504	8/26/2008	VirnetX Inc.
4 7,490,151	2/10/2009	VirnetX Inc.
5 7,921,211	4/5/2011	VirnetX Inc.

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 7,187,274		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy