Presentation of Petitioner Apple Inc.

IPR2015-00810
IPR2015-00811
IPR2015-00812

U.S. Patent No. 8,868,705
U.S. Patent No. 8,850,009

Grounds

1. IPR2015-00810

A. Ground 1: Whether Claims 1-4, 6-10, 12-26, and 28-34 are obvious under 35 U.S.C. § 103 over Beser (Beser (Ex. 1007)) and RFC 2401 (Ex. 1008)

B. Ground 2: Whether Claims 5, 11, and 27 are obvious under 35 U.S.C. § 103 over Beser, RFC 2401 and Brand (Ex. 1012)

2. IPR2015-00812

A. Ground 1: Whether Claims 1-8,10-20, and 22-25 are obvious under 35 U.S.C. § 103 over Beser (Beser (Ex. 1007)) and RFC 2401 (Ex. 1008)

IPR2015-00810, -812

1. **Beser and RFC 2401 Issues (810 & 812)**

   A. Combining Beser and RFC 2401 would have been obvious to one of ordinary skill in the art *(810 claims 1, 21) (812 claims 1, 14)*

   B. Beser and RFC 2401 teach "*a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device" (810 claims 1, 21)* (812 claims 1, 14)

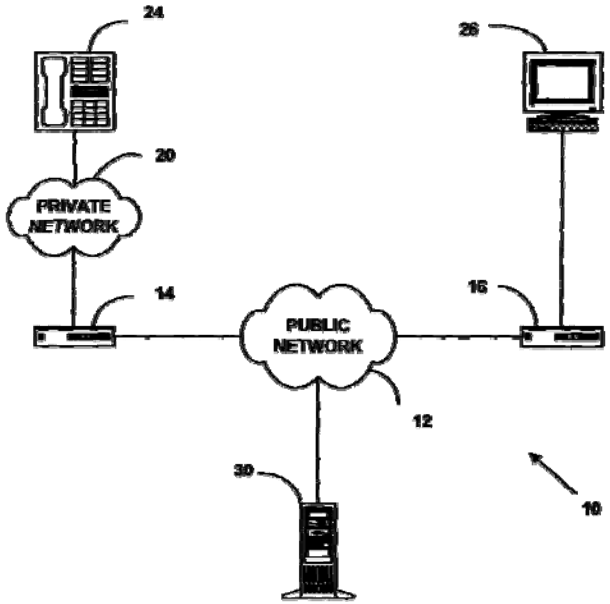
   C. Beser and RFC 2401 teach "*intercepting from the client device [the] request to look up an Internet Protocol (IP) address" (810 claims 1, 21) (812 claims 1, 14)*

2. **Beser and RFC 2401 Issues (812 only)**

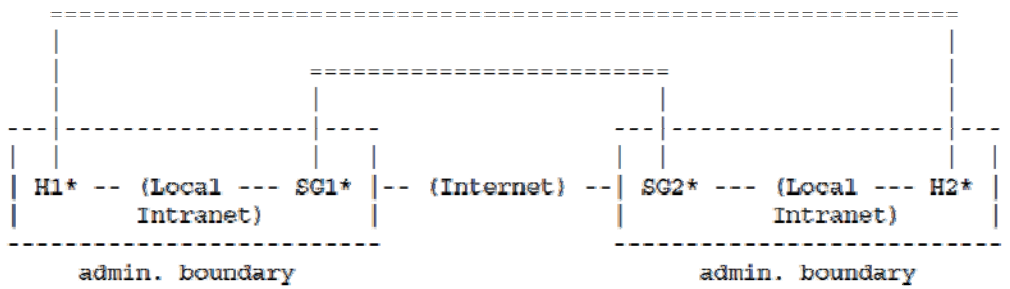
   A. Beser and RFC 2401 teach *"Receiv[ing]. . . An Indication, a Network Address, and Provisioning Information" (claims 1, 14)*

Beser and RFC 2401 Grounds

FIG. 1

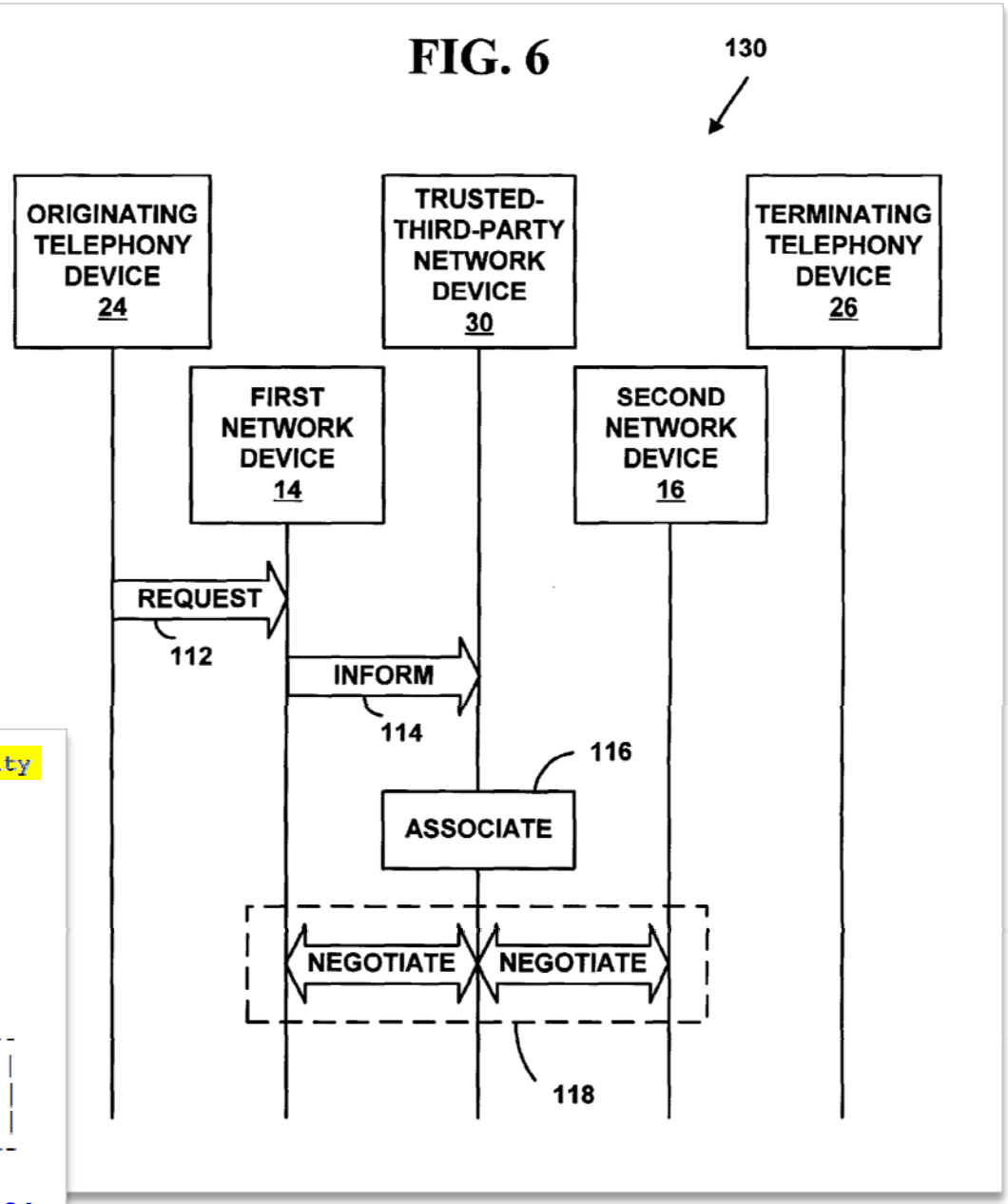


Case 3. This case combines cases 1 and 2, adding end-to-end security between the sending and receiving hosts. It imposes no new requirements on the hosts or security gateways, other than a requirement for a security gateway to be configurable to pass IPsec traffic (including ISAKMP traffic) for hosts behind it.



RFC 2401 at 25; Pet. at 24

FIG. 6



IPR2015-00810, -812

Ground 1: Beser and RFC 2401

1. **Beser and RFC 2401 Issues (810 & 812)**

   A. **Combining Beser and RFC 2401 would have been obvious to one of ordinary skill in the art *(810 claims 1, 21) (812 claims 1, 14)***

   B. Beser and RFC 2401 teach "*a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device" (810 claims 1, 21)* (812 claims 1, 14)

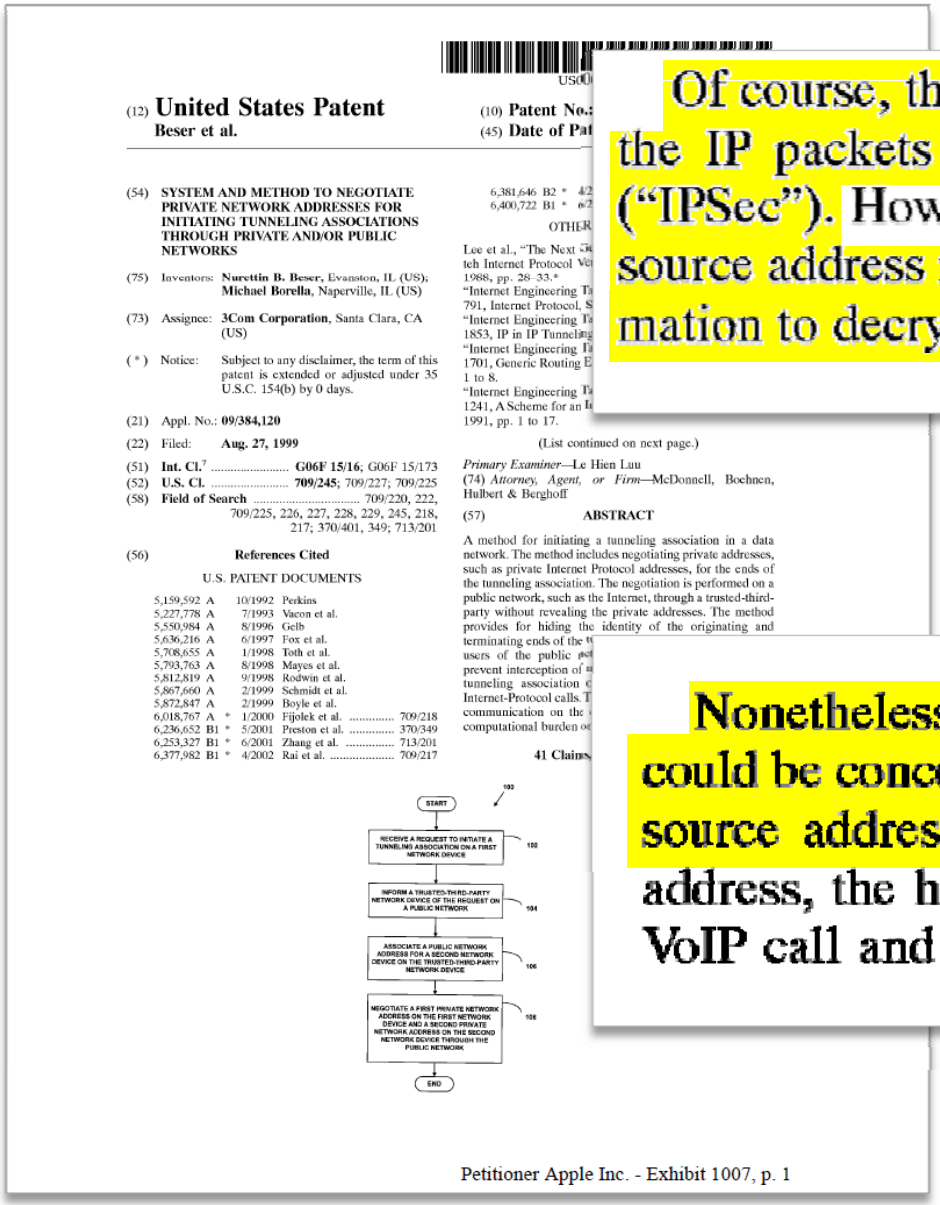
   C. Beser and RFC 2401 teach ""*intercepting from the client device [the] request to look up an Internet Protocol (IP) address" (810 claims 1, 21) (812 claims 1, 14)*

2. **Beser and RFC 2401 Issues (812 only)**

   A. Beser and RFC 2401 teach *"Receiv[ing]. . . An Indication, a Network Address, and Provisioning Information" (claims 1, 14)*

Grounds Based on Beser and RFC 2401

Combining Beser and RFC 2401



(12) **United States Patent**
Beser et al.

(10) **Patent No.:**
(45) **Date of Pat**

(54) **SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS**

(75) Inventors: **Nurettin B. Beser**, Evanston, IL (US); **Michael Borella**, Naperville, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/384,120**

(22) Filed: **Aug. 27, 1999**

(51) **Int. Cl.**[7] **G06F 15/16**; G06F 15/173
(52) **U.S. Cl.** **709/245**; 709/227; 709/225
(58) **Field of Search** 709/220, 222, 709/225, 226, 227, 228, 229, 245, 218, 217; 370/401, 349; 713/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,159,592	A	10/1992	Perkins	
5,227,778	A	7/1993	Vacon et al.	
5,550,984	A	8/1996	Gelb	
5,636,216	A	6/1997	Fox et al.	
5,708,655	A	1/1998	Toth et al.	
5,793,763	A	8/1998	Mayes et al.	
5,812,819	A	9/1998	Rodwin et al.	
5,867,660	A	2/1999	Schmidt et al.	
5,872,847	A	2/1999	Boyle et al.	
6,018,767	A *	1/2000	Fijolek et al.	709/218
6,236,652	B1 *	5/2001	Preston et al.	370/349
6,253,327	B1 *	6/2001	Zhang et al.	713/201
6,377,982	B1 *	4/2002	Rai et al.	709/217
6,381,646	B2 *	4/2		
6,400,722	B1 *	6/2		

OTHER

Lee et al., "The Next
teh Internet Protocol
1988, pp. 28–33.*
"Internet Engineering
791, Internet Protocol,
"Internet Engineering
1853, IP in IP Tunnelin
"Internet Engineering
1701, Generic Routing
1 to 8.
"Internet Engineering
1241, A Scheme for an
1991, pp. 1 to 17.

(List continued on next page.)

Primary Examiner—Le Hien Luu
(74) *Attorney, Agent, or Firm*—McDonnell, Boehnen, Hulbert & Berghoff

(57) **ABSTRACT**

A method for initiating a tunneling association in a data network. The method includes negotiating private addresses, such as private Internet Protocol addresses, for the ends of the tunneling association. The negotiation is performed on a public network, such as the Internet, through a trusted-third-party without revealing the private addresses. The method provides for hiding the identity of the originating and terminating ends of the
users of the public
prevent interception of
tunneling association
Internet-Protocol calls.
communication on the
computational burden

41 Claims

Petitioner Apple Inc. - Exhibit 1007, p. 1

Of course, the sender may encrypt the information inside the IP packets before transmission, e.g. with IP Security ("IPSec"). However, accumulating all the packets from one source address may provide the hacker with sufficient information to decrypt the message. Moreover, encryption at the

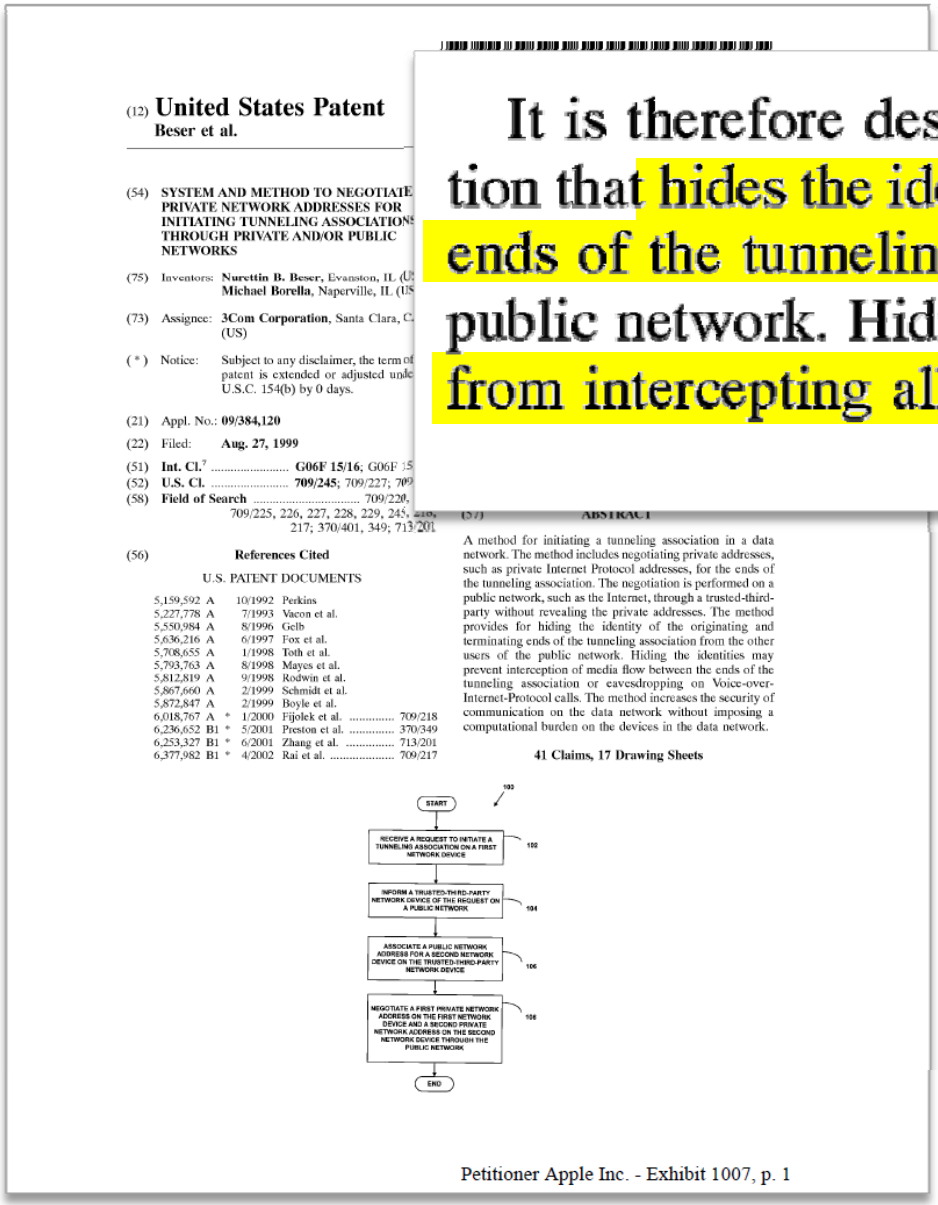
Beser (Ex. 1007) at 1:54-58; Pet. (810) at 22, 24

Nonetheless, even if the information inside the IP packets could be concealed, the hacker is still capable of reading the source address of the packets. Armed with the source IP address, the hacker may have the capability of tracing any VoIP call and eavesdropping on all calls from that source.

Beser (Ex. 1007) at 2:1-5; Reply (810) at 4

Grounds Based on Beser and RFC 2401

Combining Beser and RFC 2401



(12) **United States Patent**
Beser et al.

(54) **SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS**

(75) Inventors: **Nurettin B. Beser**, Evanston, IL (US); **Michael Borella**, Naperville, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/384,120**

(22) Filed: **Aug. 27, 1999**

(51) **Int. Cl.**[7] **G06F 15/16**; G06F 15/

(52) **U.S. Cl.** **709/245**; 709/227; 709/

(58) **Field of Search** 709/220, 709/225, 226, 227, 228, 229, 245, 217; 370/401, 349; 713/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,159,592	A		10/1992	Perkins
5,227,778	A		7/1993	Vacon et al.
5,550,984	A		8/1996	Gelb
5,636,216	A		6/1997	Fox et al.
5,708,655	A		1/1998	Toth et al.
5,793,763	A		8/1998	Mayes et al.
5,812,819	A		9/1998	Rodwin et al.
5,867,660	A		2/1999	Schmidt et al.
5,872,847	A		2/1999	Boyle et al.
6,018,767	A	*	1/2000	Fijolek et al. 709/218
6,236,652	B1	*	5/2001	Preston et al. 370/349
6,253,327	B1	*	6/2001	Zhang et al. 713/201
6,377,982	B1	*	4/2002	Rai et al. 709/217

(57) **ABSTRACT**

A method for initiating a tunneling association in a data network. The method includes negotiating private addresses, such as private Internet Protocol addresses, for the ends of the tunneling association. The negotiation is performed on a public network, such as the Internet, through a trusted-third-party without revealing the private addresses. The method provides for hiding the identity of the originating and terminating ends of the tunneling association from the other users of the public network. Hiding the identities may prevent interception of media flow between the ends of the tunneling association or eavesdropping on Voice-over-Internet-Protocol calls. The method increases the security of communication on the data network without imposing a computational burden on the devices in the data network.

41 Claims, 17 Drawing Sheets

Petitioner Apple Inc. - Exhibit 1007, p. 1

It is therefore desirable to establish a tunneling association that hides the identity of the originating and terminating ends of the tunneling association from the other users of a public network. Hiding the identities may prevent a hacker from intercepting all media flow between the ends.

Beser (Ex. 1007) at 2:36-40; Reply (810) at 5

Combining Beser and RFC 2401

UNITED STATES PATENT AND TR

BEFORE THE PATENT TRIAL AN

APPLE INC.
Petitioner,

v.

VIRNETX, INC. AND SCIENCE APPLICA
CORPORATION
Patent Owner.

Patent No. 8,868,7
Issued: October 21, 2
Filed: September 13, 2
Inventors: Victor Larson
Title: AGILE NETWORK PROTOCOL FOR SE
USING SECURE DOMAIN

Inter Partes Review No. IPR

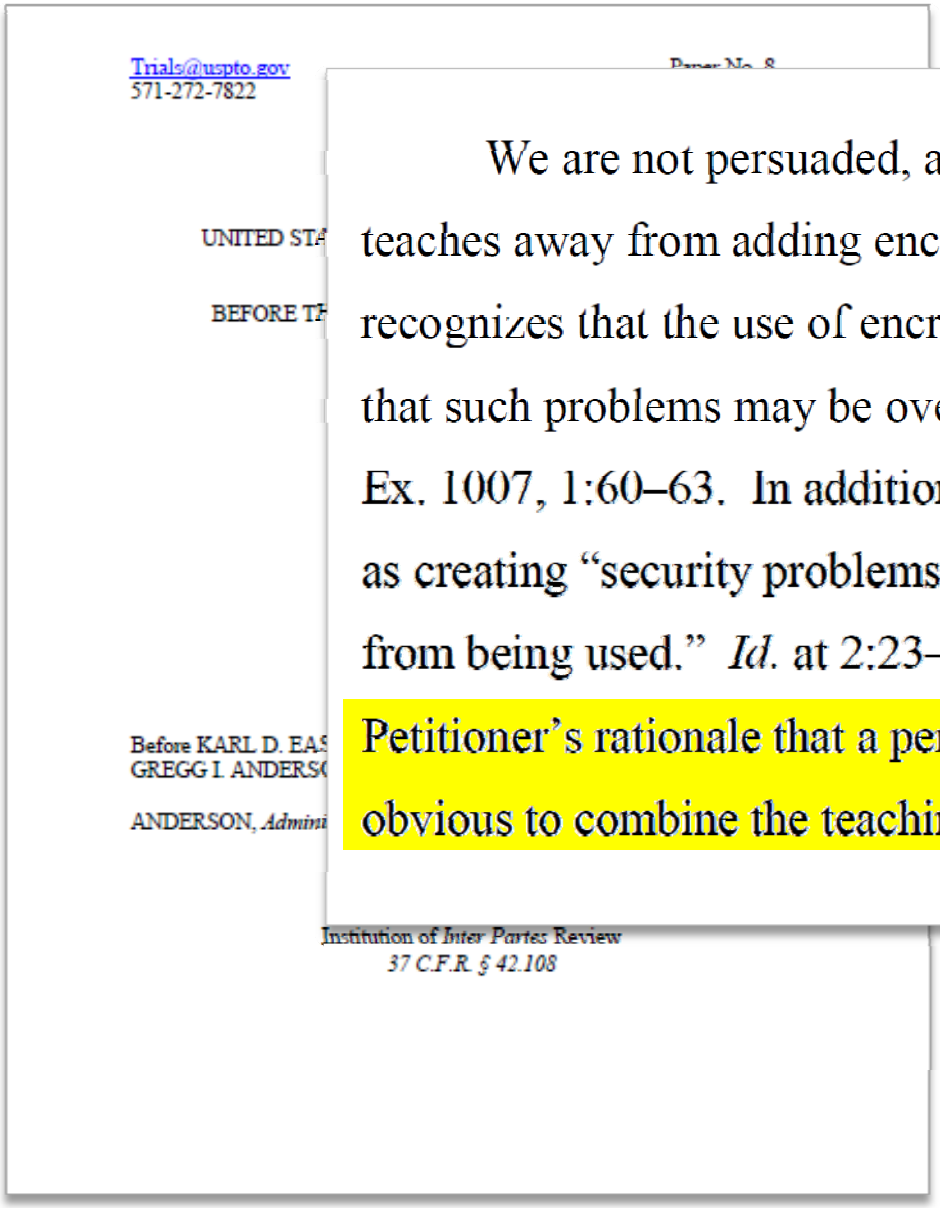
Petition for *Inter Partes* R
U.S. Patent No. 8,868

A person of ordinary skill also would have also recognized IPsec could be readily integrated into the Beser systems. Ex. 1005 at ¶¶ 391-92, 398-400. For example, Beser describes systems that use edge routers and gateways as intermediaries in transmitting traffic over tunneling associations, which is one of the network designs shown in RFC 2401. Ex. 1007 at 4:7-8, 4:18-29. Indeed, RFC 2401 in its "case 3" example shows precisely the same network topology as Beser, with one tunnel between two security gateways such as edge routers, and another tunnel between the two end devices. *Compare* Ex. 1008 at 25 *with* Ex. 1007 at Fig. 1; Ex. 1005 at ¶¶ 396-97. When Beser is configured in this manner, it would use the IPSec case 3 design to provide end-to-end encryption, hiding the data, while the Beser IP tunnel would provide anonymity over the public network, hiding the true source and destination addresses. Ex. 1005 at ¶ 399.

Pet. (810) at 28

Institution Decision

Combining Beser and RFC 2401


Trials@uspto.gov
571-272-7822

UNITED STA

BEFORE TH

Before KARL D. EAS
GREGG I. ANDERS

ANDERSON, *Admini*

Institution of *Inter Partes* Review
37 C.F.R. § 42.108

We are not persuaded, at this point in the proceeding that Beser teaches away from adding encryption to its system. Although Beser recognizes that the use of encryption may cause challenges, it also suggests that such problems may be overcome by providing more computer power. Ex. 1007, 1:60–63. In addition, Beser characterizes some prior art systems as creating "security problems by preventing certain types of encryption from being used." *Id.* at 2:23–24. We are, therefore, persuaded that Petitioner's rationale that a person of ordinary skill would have found it obvious to combine the teachings of RFC 2401 with Beser is reasonable.

Decision (810) at 13

Patent Owner Assertion

Combining Beser and RFC 2401

Filed on behalf of: Vir
By:
Joseph E. Palys
Paul Hastings LLP
875 15th Street NW
Washington, DC 2000
Telephone: (202) 551-
Facsimile: (202) 551-
E-mail: josephpalys@

UNITED ST

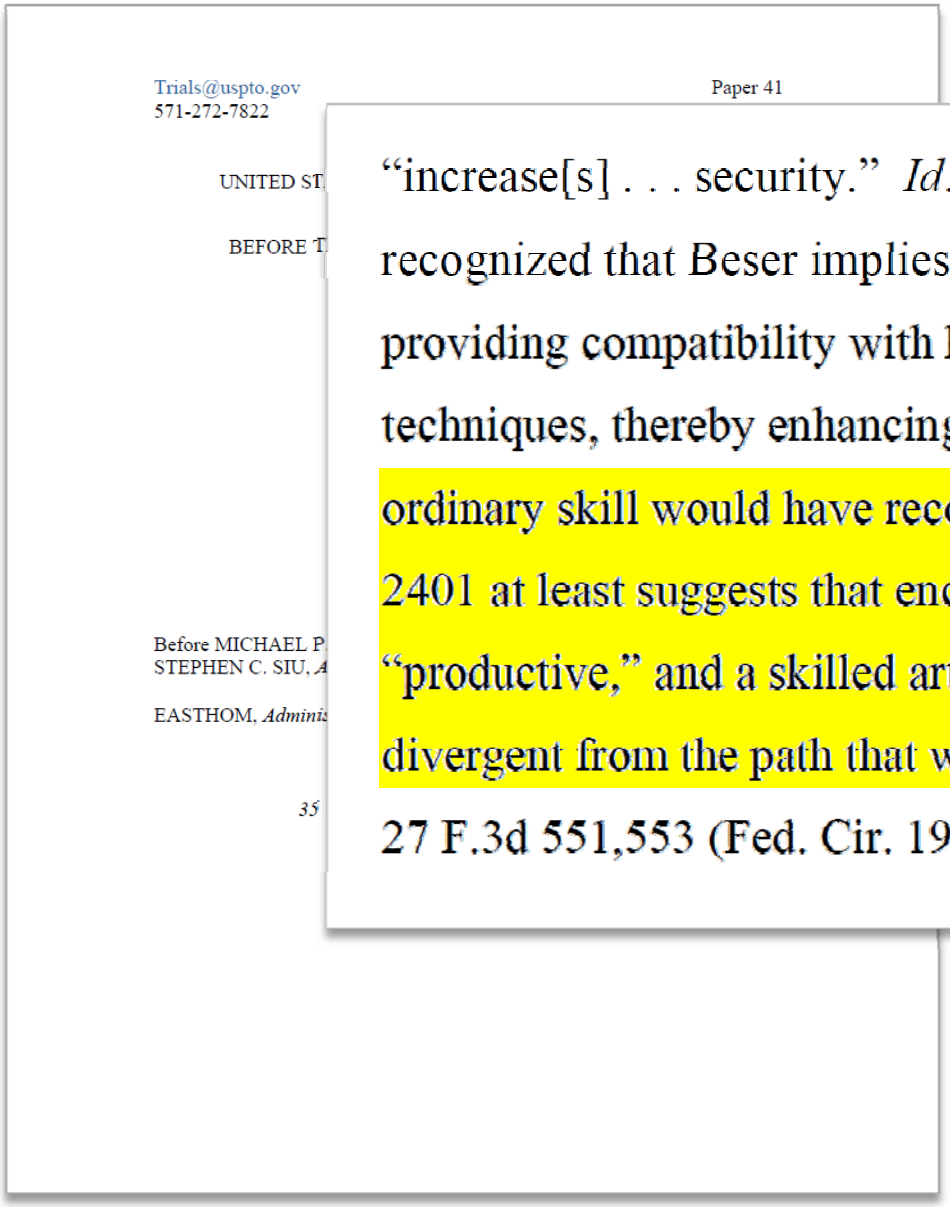
BEFORE T

Given the teachings of *Beser*, a person of ordinary skill in the art "would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path [in RFC 2401]." *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994); (*See, e.g.*, Ex. 2016 at ¶¶ 40-48.). *Beser* does not merely disclose two alternatives, one of which is the claimed alternative. Rather, *Beser's* disclosure "criticize[s], discredit[s], or otherwise discourage[s]" the use of encryption for communication over the Internet. *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004). In fact, the entirety of the *Beser* disclosure is directed to overcoming the problems of and providing a solution to the prior art use of encryption to secure communications over the Internet.

Opposition (810) at 32

Final Written Decision in IPR2014-00237

Combining Beser and RFC 2401


Trials@uspto.gov
571-272-7822

Paper 41

UNITED ST

BEFORE T

Before MICHAEL P
STEPHEN C. SIU, *A*

EASTHOM, *Adminis*

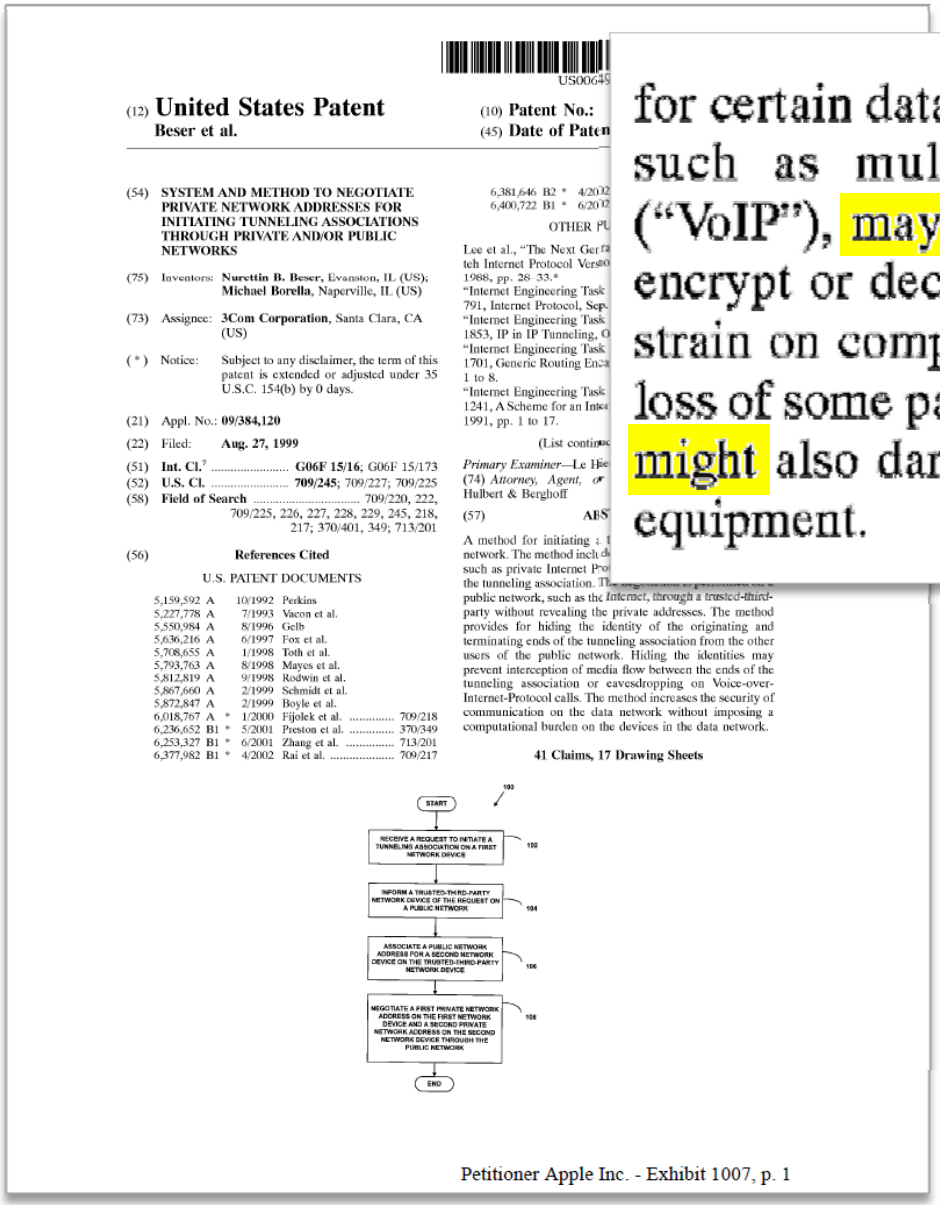
35

"increase[s] . . . security." *Id.* at 3:7. Therefore, skilled artisans would have recognized that Beser implies or suggests solving these security problems by providing compatibility with known audio or video data encryption techniques, thereby enhancing security. The record shows that artisans of ordinary skill would have recognized that the combination of Beser and RFC 2401 at least suggests that encrypting audio or video likely would be "productive," and a skilled artisan "would [not] be led in a direction divergent from the path that was taken by the applicant." *See In re Gurley*, 27 F.3d 551,553 (Fed. Cir. 1994).

Final Written Decision, IPR2014-00237 at 41; Reply (810) at 2-3

Grounds Based on Beser and RFC 2401

Combining Beser and RFC 2401



US006[illegible]

(12) **United States Patent**
Beser et al.

(10) **Patent No.:**
(45) **Date of Paten**

(54) **SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS**

(75) Inventors: **Nurettin B. Beser**, Evanston, IL (US); **Michael Borella**, Naperville, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/384,120**

(22) Filed: **Aug. 27, 1999**

(51) **Int. Cl.**[7] **G06F 15/16**; G06F 15/173
(52) **U.S. Cl.** **709/245**; 709/227; 709/225
(58) **Field of Search** 709/220, 222, 709/225, 226, 227, 228, 229, 245, 218, 217; 370/401, 349; 713/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,159,592	A	10/1992	Perkins	
5,227,778	A	7/1993	Vacon et al.	
5,550,984	A	8/1996	Gelb	
5,636,216	A	6/1997	Fox et al.	
5,708,655	A	1/1998	Toth et al.	
5,793,763	A	8/1998	Mayes et al.	
5,812,819	A	9/1998	Rodwin et al.	
5,867,660	A	2/1999	Schmidt et al.	
5,872,847	A	2/1999	Boyle et al.	
6,018,767	A *	1/2000	Fijolek et al.	709/218
6,236,652	B1 *	5/2001	Preston et al.	370/349
6,253,327	B1 *	6/2001	Zhang et al.	713/201
6,377,982	B1 *	4/2002	Rai et al.	709/217
6,381,646	B2 *	4/2002		
6,400,722	B1 *	6/2002		

OTHER PU

Lee et al., "The Next Ger
teh Internet Protocol Vers
1988, pp. 28–33.*
"Internet Engineering Task
791, Internet Protocol, Sep.
"Internet Engineering Task
1853, IP in IP Tunneling, O
"Internet Engineering Task
1701, Generic Routing Enca
1 to 8.
"Internet Engineering Task
1241, A Scheme for an Inte
1991, pp. 1 to 17.

(List continu

Primary Examiner—Le Hie
(74) *Attorney, Agent, or*
Hulbert & Berghoff

(57) ABS

A method for initiating a
network. The method incl
such as private Internet Pro
the tunneling association. T
public network, such as the *Internet*, through a *trusted-third-party* without revealing the private addresses. The method provides for hiding the identity of the originating and terminating ends of the tunneling association from the other users of the public network. Hiding the identities may prevent interception of media flow between the ends of the tunneling association or eavesdropping on Voice-over-Internet-Protocol calls. The method increases the security of communication on the data network without imposing a computational burden on the devices in the data network.

41 Claims, 17 Drawing Sheets

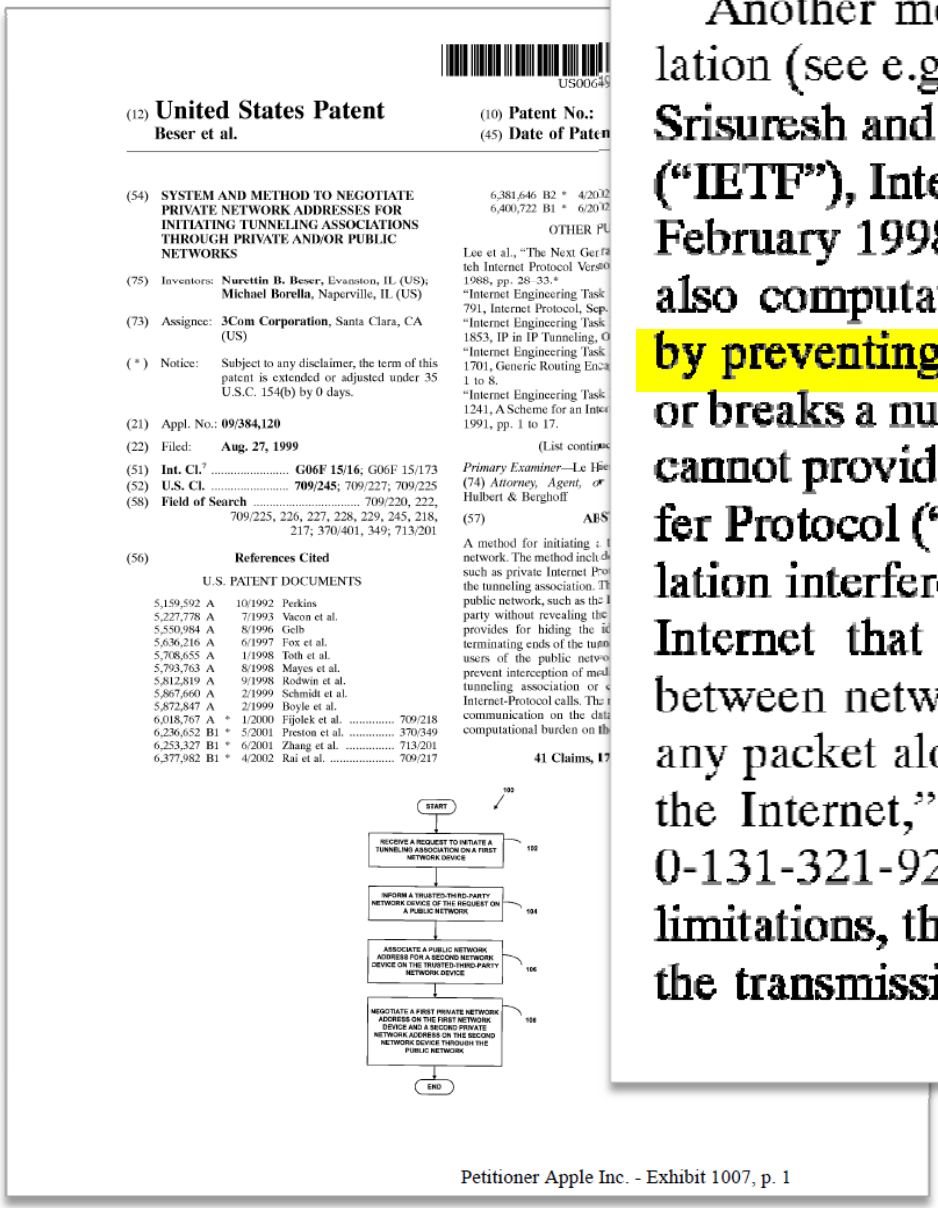
Petitioner Apple Inc. - Exhibit 1007, p. 1

for certain data formats. For example, streaming data flows, such as multimedia or Voice-over-Internet-Protocol ("VoIP"), may require a great deal of computing power to encrypt or decrypt the IP packets on the fly. The increased strain on computer power may result in jitter, delay, or the loss of some packets. The expense of added computer power might also dampen the customer's desire to invest in VoIP equipment.

Beser (Ex. 1007) at 1:60-67; Pet. (810) at 24; Reply (810) at 6

Grounds Based on Beser and RFC 2401

Combining Beser and RFC 2401



(12) **United States Patent**
Beser et al.

(10) **Patent No.:**
(45) **Date of Paten**

(54) **SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS**

(75) Inventors: **Nurettin B. Beser**, Evanston, IL (US); **Michael Borella**, Naperville, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/384,120**

(22) Filed: **Aug. 27, 1999**

(51) **Int. Cl.**[7] **G06F 15/16**; G06F 15/173
(52) **U.S. Cl.** **709/245**; 709/227; 709/225
(58) **Field of Search** 709/220, 222, 709/225, 226, 227, 228, 229, 245, 218, 217; 370/401, 349; 713/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,159,592	A	10/1992	Perkins	
5,227,778	A	7/1993	Vacon et al.	
5,550,984	A	8/1996	Gelb	
5,636,216	A	6/1997	Fox et al.	
5,708,655	A	1/1998	Toth et al.	
5,793,763	A	8/1998	Mayes et al.	
5,812,819	A	9/1998	Rodwin et al.	
5,867,660	A	2/1999	Schmidt et al.	
5,872,847	A	2/1999	Boyle et al.	
6,018,767	A *	1/2000	Fijolek et al.	709/218
6,236,652	B1 *	5/2001	Preston et al.	370/349
6,253,327	B1 *	6/2001	Zhang et al.	713/201
6,377,982	B1 *	4/2002	Rai et al.	709/217
6,381,646	B2 *	4/2002		
6,400,722	B1 *	6/2002		

OTHER PU

Lee et al., "The Next Ger
teh Internet Protocol Vers
1988, pp. 28–33.*
"Internet Engineering Task
791, Internet Protocol, Sep.
"Internet Engineering Task
1853, IP in IP Tunneling, O
"Internet Engineering Task
1701, Generic Routing Enca
1 to 8.
"Internet Engineering Task
1241, A Scheme for an Inte
1991, pp. 1 to 17.

(List continu

Primary Examiner—Le Hie
(74) *Attorney, Agent, or*
Hulbert & Berghoff

(57) ABS

A method for initiating a t
network. The method incl
such as private Internet Pro
the tunneling association. Th
public network, such as the
party without revealing the
provides for hiding the id
terminating ends of the tun
users of the public netwo
prevent interception of mes
tunneling association or
Internet-Protocol calls. The
communication on the data
computational burden on th

41 Claims, 17

Petitioner Apple Inc. - Exhibit 1007, p. 1

Another method for tunneling is network address translation (see e.g., "The IP Network Address Translator", by P. Srisuresh and K. Egevang, Internet Engineering Task Force ("IETF"), Internet Draft <draft-rfced-info-srisuresh-05.txt>, February 1998). However, this type of address translation is also computationally expensive, causes security problems by preventing certain types of encryption from being used, or breaks a number of existing applications in a network that cannot provide network address translation (e.g., File Transfer Protocol ("FTP")). What is more, network address translation interferes with the end-to-end routing principal of the Internet that recommends that packets flow end-to-end between network devices without changing the contents of any packet along a transmission route (see e.g., "Routing in the Internet," by C. Huitema, Prentice Hall, 1995, ISBN 0-131-321-927). Once again, due to computer power limitations, this form of tunneling may be inappropriate for the transmission of multimedia or VoIP packets.

Beser (Ex. 1007) at 2:18-35; Pet. (810) at 29; Reply (810) at 4

IPR2015-00810, -812

Ground 1: Beser and RFC 2401

1. **Beser and RFC 2401 Issues (810 & 812)**

   A. Combining Beser and RFC 2401 would have been obvious to one of ordinary skill in the art *(810 claims 1, 21) (812 claims 1, 14)*

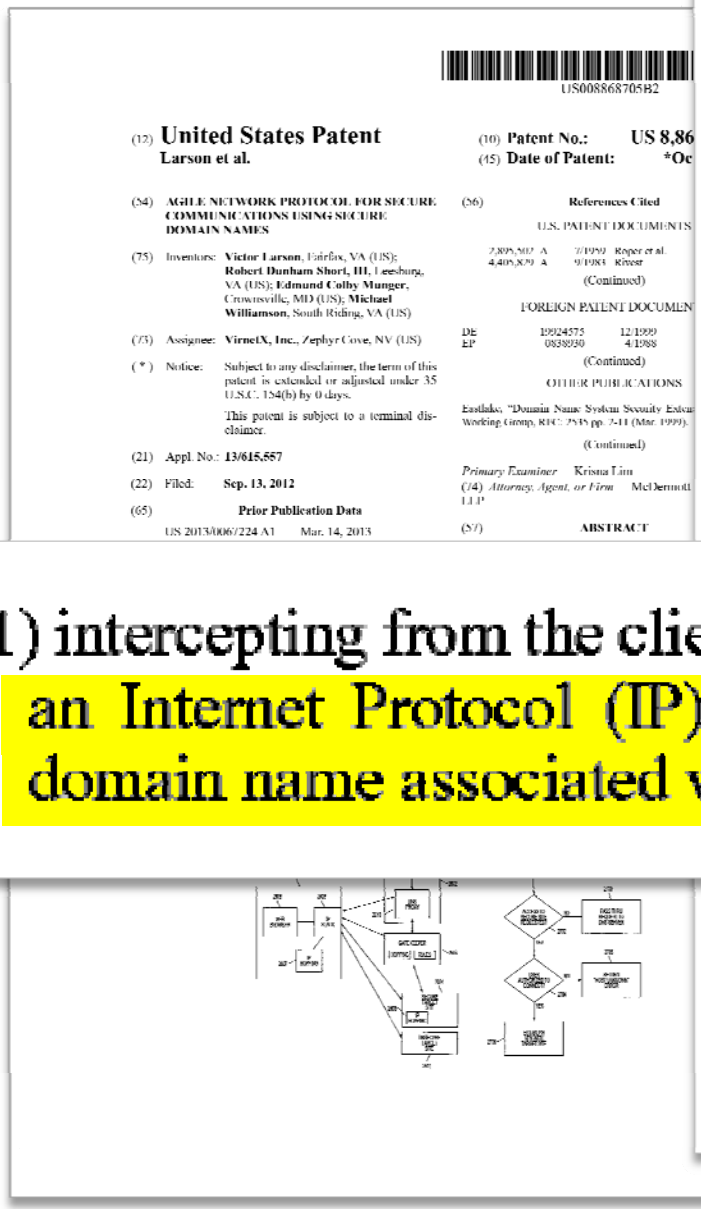
   B. Beser and RFC 2401 teach "*a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device*" *(810 claims 1, 21)* (812 claims 1, 14)

   C. Beser and RFC 2401 teach "*intercepting from the client device [the] request to look up an Internet Protocol (IP) address*" *(810 claims 1, 21) (812 claims 1, 14)*

2. **Beser and RFC 2401 Issues (812 only)**

   A. Beser and RFC 2401 teach *"Receiv[ing]. . . An Indication, a Network Address, and Provisioning Information" (claims 1, 14)*

’705 Patent, Claim 1



US008868705B2

(12) **United States Patent**
Larson et al.

(10) **Patent No.: US 8,86**
(45) **Date of Patent: *Oc**

(54) **AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmund Colby Munger**, Crownsville, MD (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **VirnetX, Inc.**, Zephyr Cove, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/615,557**

(22) Filed: **Sep. 13, 2012**

(65) **Prior Publication Data**

US 2013/0067224 A1 Mar. 14, 2013

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,305,537 A 7/1999 Roper et al.
4,405,829 A 9/1983 Rivest

(Continued)

FOREIGN PATENT DOCUMEN

DE 19924575 12/1999
EP 0838930 4/1988

(Continued)

OTHER PUBLICATIONS

Eastlake, "Domain Name System Security Exten
Working Group, RFC 2535 pp. 7-11 (Mar. 1999).

(Continued)

Primary Examiner Krisna Lim
(74) *Attorney, Agent, or Firm* McDermott
LLP

(57) **ABSTRACT**

1. A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the

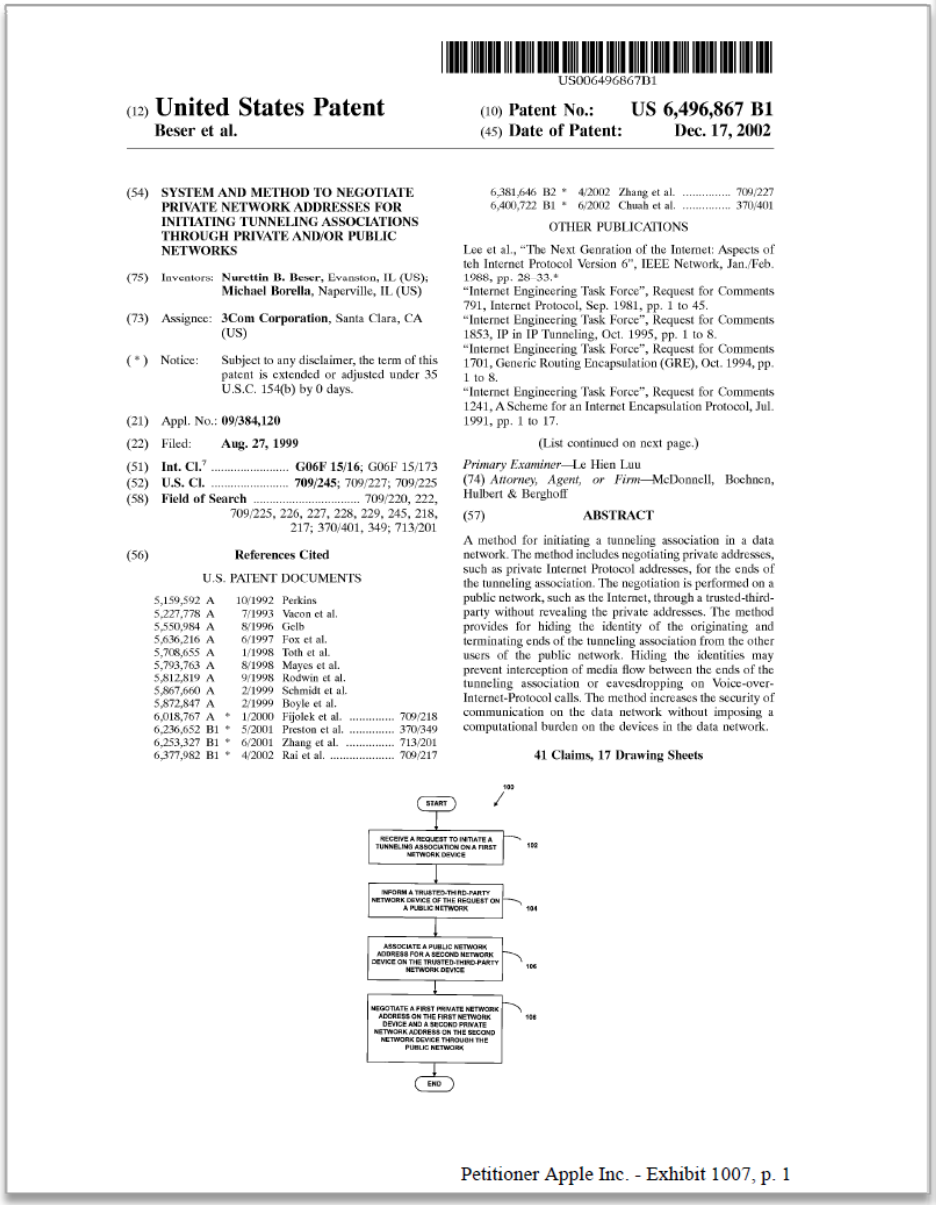
hat the request
responds to a
ications chan-
oviding provi-
he creation of
tween the cli-
ent device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel.

’705 Patent (Ex. 1001) at Claim 1

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

Grounds Based on Beser and RFC 2401

Combining Beser and RFC 2401



US006496867B1

(12) **United States Patent**
Beser et al.

(10) **Patent No.: US 6,496,867 B1**
(45) **Date of Patent: Dec. 17, 2002**

(54) **SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS**

(75) Inventors: **Nurettin B. Beser**, Evanston, IL (US); **Michael Borella**, Naperville, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/384,120**

(22) Filed: **Aug. 27, 1999**

(51) **Int. Cl.**[7] **G06F 15/16**; G06F 15/173
(52) **U.S. Cl.** **709/245**; 709/227; 709/225
(58) **Field of Search** 709/220, 222, 709/225, 226, 227, 228, 229, 245, 218, 217; 370/401, 349; 713/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,159,592	A		10/1992	Perkins
5,227,778	A		7/1993	Vacon et al.
5,550,984	A		8/1996	Gelb
5,636,216	A		6/1997	Fox et al.
5,708,655	A		1/1998	Toth et al.
5,793,763	A		8/1998	Mayes et al.
5,812,819	A		9/1998	Rodwin et al.
5,867,660	A		2/1999	Schmidt et al.
5,872,847	A		2/1999	Boyle et al.
6,018,767	A	*	1/2000	Fijolek et al. 709/218
6,236,652	B1	*	5/2001	Preston et al. 370/349
6,253,327	B1	*	6/2001	Zhang et al. 713/201
6,377,982	B1	*	4/2002	Rai et al. 709/217
6,381,646	B2	*	4/2002	Zhang et al. 709/227
6,400,722	B1	*	6/2002	Chuah et al. 370/401

OTHER PUBLICATIONS

Lee et al., "The Next Genration of the Internet: Aspects of teh Internet Protocol Version 6", IEEE Network, Jan./Feb. 1988, pp. 28–33.*
"Internet Engineering Task Force", Request for Comments 791, Internet Protocol, Sep. 1981, pp. 1 to 45.
"Internet Engineering Task Force", Request for Comments 1853, IP in IP Tunneling, Oct. 1995, pp. 1 to 8.
"Internet Engineering Task Force", Request for Comments 1701, Generic Routing Encapsulation (GRE), Oct. 1994, pp. 1 to 8.
"Internet Engineering Task Force", Request for Comments 1241, A Scheme for an Internet Encapsulation Protocol, Jul. 1991, pp. 1 to 17.

(List continued on next page.)

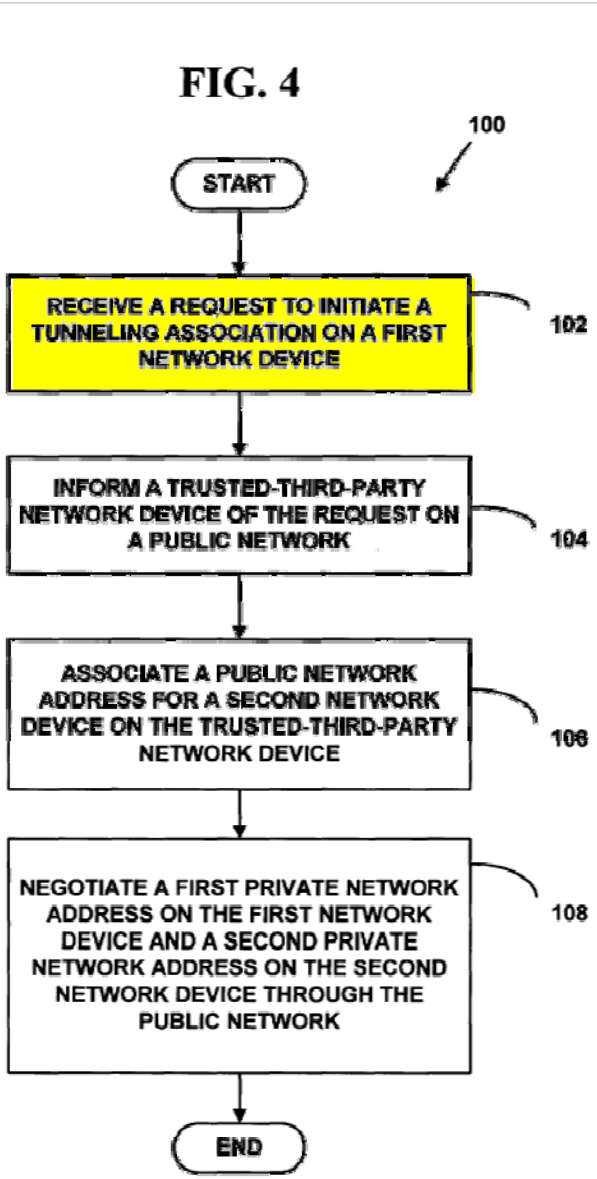
Primary Examiner—Le Hien Luu
(74) *Attorney, Agent, or Firm*—McDonnell, Boehnen, Hulbert & Berghoff

(57) **ABSTRACT**

A method for initiating a tunneling association in a data network. The method includes negotiating private addresses, such as private Internet Protocol addresses, for the ends of the tunneling association. The negotiation is performed on a public network, such as the Internet, through a trusted-third-party without revealing the private addresses. The method provides for hiding the identity of the originating and terminating ends of the tunneling association from the other users of the public network. Hiding the identities may prevent interception of media flow between the ends of the tunneling association or eavesdropping on Voice-over-Internet-Protocol calls. The method increases the security of communication on the data network without imposing a computational burden on the devices in the data network.

41 Claims, 17 Drawing Sheets

Petitioner Apple Inc. - Exhibit 1007, p. 1



Beser (Ex. 1007) at Fig. 4; Pet. (810) at 43

Beser and RFC 2401

"a request to look up an Internet Protocol (IP) address"

UNITED STATES PATENT AND TRADEMAR

BEFORE THE PATENT TRIAL AND APPEAL

APPLE INC.
Petitioner,

v.

VIRNETX, INC. AND SCIENCE APPLICATION IN
CORPORATION,
Patent Owner.

Patent No. 8,868,705
Issued: October 21, 2014
Filed: September 13, 2012
Inventors: Victor Larson, *et al.*
Title: AGILE NETWORK PROTOCOL FOR SECURE
USING SECURE DOMAIN NAMES

Inter Partes Review No. IPR2015-00

Petition for *Inter Partes* Review of U.S. Patent No. 8,868,705

Beser also explains that, in response to the request, the trusted-third-party network device will look up and return to the first network device a public IP address for the second network device and a private IP address for the terminating device ("*a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device*"). Ex. 1007 at 11:26-36, 12:28-32, 14:19-27, 17:42-49; Ex. 1005 at ¶¶ 310, 339. Therefore, Beser shows a system and method that perform the first step specified in **claims 1 and 21**.

Pet. at 34

310. When the trusted-third-party network device receives a request to initiate a tunneling association, it uses the unique identifier in the request to look-up the corresponding IP address in its database of registered unique identifiers. Ex. 1007 (Beser) at 11:26-36, 11:45-55. To initiate the secure IP tunnel, the trusted-third-party network device will look-up the IP address of the corresponding second network device. Ex. 1007 (Beser) at 9:6-8, 11:26-36.

Ex. 1005 at ¶ 310; Pet. (810) at 33

Patent Owner Assertion

"a request to look up an Internet Protocol (IP) address"

Filed on behalf of: Vir
By:
Joseph E. Palys
Paul Hastings LLP
875 15th Street NW
Washington, DC 2000
Telephone: (202) 551-
Facsimile: (202) 551-
E-mail: josephpalys@

UNITED ST

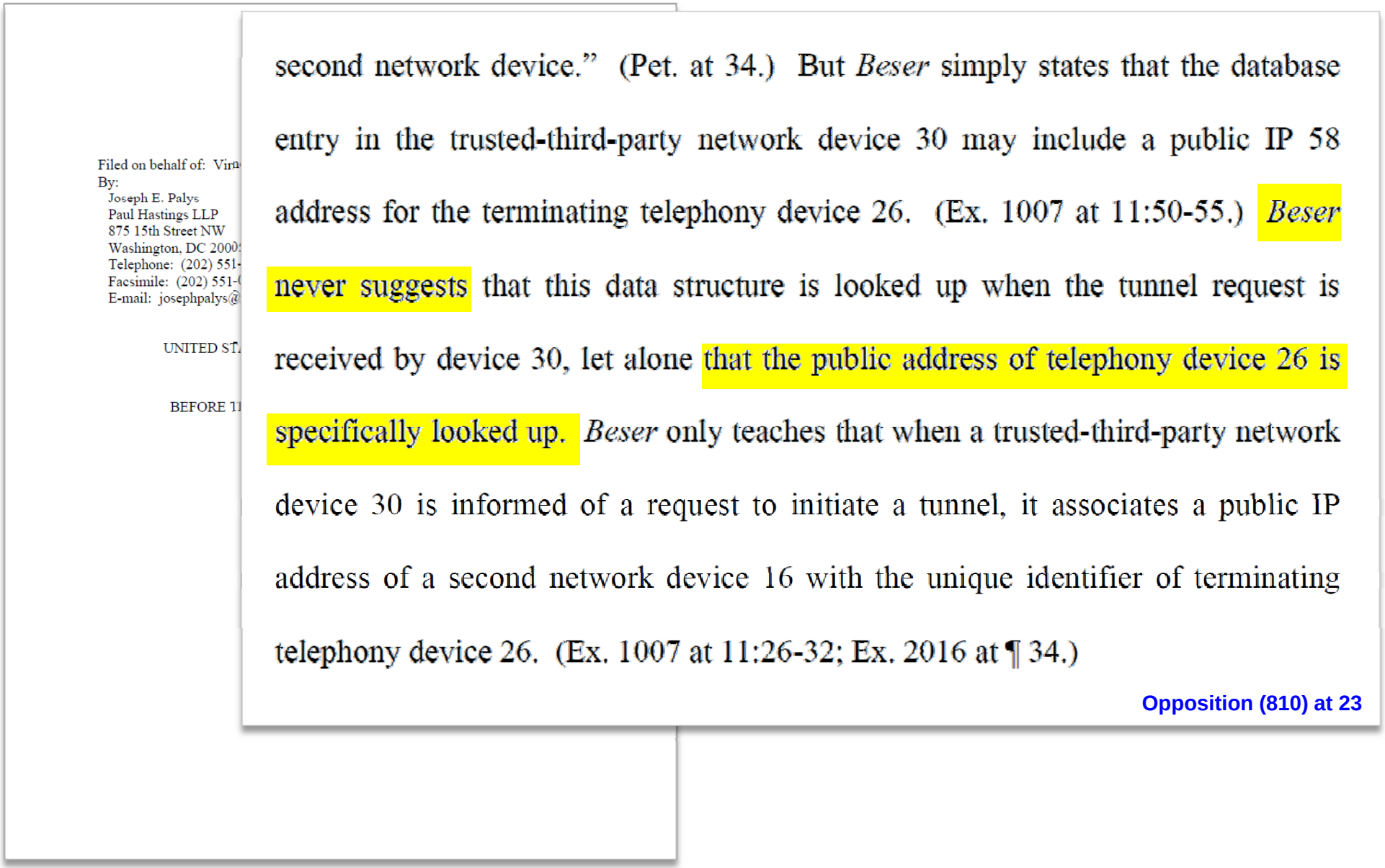
BEFORE T

second network device." (Pet. at 34.) But *Beser* simply states that the database entry in the trusted-third-party network device 30 may include a public IP 58 address for the terminating telephony device 26. (Ex. 1007 at 11:50-55.) *Beser* never suggests that this data structure is looked up when the tunnel request is received by device 30, let alone that the public address of telephony device 26 is specifically looked up. *Beser* only teaches that when a trusted-third-party network device 30 is informed of a request to initiate a tunnel, it associates a public IP address of a second network device 16 with the unique identifier of terminating telephony device 26. (Ex. 1007 at 11:26-32; Ex. 2016 at ¶ 34.)

Opposition (810) at 23

Patent Owner Assertion

"a request to look up an Internet Protocol (IP) address"



Filed on behalf of: Vir
By:
Joseph E. Palys
Paul Hastings LLP
875 15th Street NW
Washington, DC 2000
Telephone: (202) 551-
Facsimile: (202) 551-
E-mail: josephpalys@

UNITED ST

BEFORE T

second network device." (Pet. at 34.) But *Beser* simply states that the database entry in the trusted-third-party network device 30 may include a public IP 58 address for the terminating telephony device 26. (Ex. 1007 at 11:50-55.) *Beser* never suggests that this data structure is looked up when the tunnel request is received by device 30, let alone that the public address of telephony device 26 is specifically looked up. *Beser* only teaches that when a trusted-third-party network device 30 is informed of a request to initiate a tunnel, it associates a public IP address of a second network device 16 with the unique identifier of terminating telephony device 26. (Ex. 1007 at 11:26-32; Ex. 2016 at ¶ 34.)

Opposition (810) at 23

Grounds Based on Beser and RFC 2401

"a request to look up an Internet Protocol (IP) address"

US006496867B1

(12) **United States Patent**
Beser et al.

(10) **Patent No.: US 6,496,867 B1**
(45) **Date of Patent: Dec. 17, 2002**

(54) **SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS**

(75) Inventors: **Nurettin B. Beser**, Evanston, IL (US); **Michael Borella**, Naperville, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/384,120**

(22) Filed: **Aug. 27, 1999**

(51) **Int. Cl.**[7] **G06F 15/16**; G06F 15/173

(52) **U.S. Cl.** **709/245**; 709/227; 709/225

(58) **Field of Search** 709/220, 222, 709/225, 226, 227, 228, 229, 245, 218, 217; 370/401, 349; 713/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,159,592	A	10/1992	Perkins	
5,227,778	A	7/1993	Vacon et al.	
5,550,984	A	8/1996	Gelb	
5,636,216	A	6/1997	Fox et al.	
5,708,655	A	1/1998	Toth et al.	
5,793,763	A	8/1998	Mayes et al.	
5,812,819	A	9/1998	Rodwin et al.	
5,867,660	A	2/1999	Schmidt et al.	
5,872,847	A	2/1999	Boyle et al.	
6,018,767	A *	1/2000	Fijolek et al.	709/218
6,236,652	B1 *	5/2001	Preston et al.	370/349
6,253,327	B1 *	6/2001	Zhang et al.	713/201
6,377,982	B1 *	4/2002	Rai et al.	709/217
6,381,646	B2 *	4/2002	Zhang et al.	709/227
6,400,722	B1 *	6/2002	Chuah et al.	370/401

OTHER PUBLICATIONS

Lee et al., "The Next Genration of the Internet: Aspects of teh Internet Protocol Version 6", IEEE Network, Jan./Feb. 1988, pp. 28–33.*
"Internet Engineering Task Force", Request for Comments 791, Internet Protocol, Sep. 1981, pp. 1 to 45.
"Internet Engineering Task Force", Request for Comments 1853, IP in IP Tunneling, Oct. 1995, pp. 1 to 8.
"Internet Engineering Task Force", Request for Comments 1701, Generic Routing Encapsulation (GRE), Oct. 1994, pp. 1 to 8.
"Internet Engineering Task Force", Request for Comments 1241, A Scheme for an Internet Encapsulation Protocol, Jul. 1991, pp. 1 to 17.

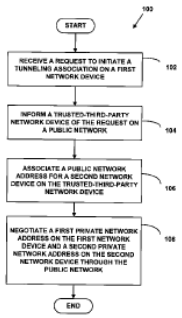
(List continued on next page.)

Primary Examiner—Le Hien Luu
(74) *Attorney, Agent, or Firm*—McDonnell, Boehnen, Hulbert & Berghoff

(57) **ABSTRACT**

A method for initiating a tunneling association in a data network. The method includes negotiating private addresses, such as private Internet Protocol addresses, for the ends of the tunneling association. The negotiation is performed on a public network, such as the Internet, through a trusted-third-party without revealing the private addresses. The method provides for hiding the identity of the originating and terminating ends of the tunneling association from the other users of the public network. Hiding the identities may prevent interception of media flow between the ends of the tunneling association or eavesdropping on Voice-over-Internet-Protocol calls. The method increases the security of communication on the data network without imposing a computational burden on the devices in the data network.

41 Claims, 17 Drawing Sheets



Petitioner Apple Inc. - Exhibit 1007, p. 1

A public IP **58** address for a second network device **16** is associated with the unique identifier for the terminating telephony device **26** at Step **116**. The second network device **16** is associated with the terminating telephony device **26**. This association of the public IP **58** address for the second network device **16** with the unique identifier is made on the trusted-third-party network device **30**. In one exemplary preferred embodiment, the trusted-third-party network device **30** is a back-end service, a domain name server, or the owner/manager of database or directory services and may be distributed over several physical locations. In another exem-

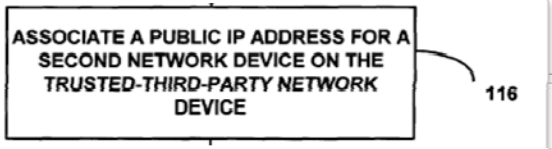
* * *

For example, the trusted-third-party network device **30** may be a directory service, owned and operated by a telephone company, that retains a list of E.164 numbers of its subscribers. Associated with a E.164 number in the directory database is the IP **58** address of a particular second network device **16**. The database entry may also include a public IP **58** addresses for the terminating telephony device **26**. Many data structures that are known to those skilled in the art are possible for the association of the unique identifiers and IP **58** addresses for the second network devices **16**. However, it should be understood that the present invention is not restricted to E.164 telephone numbers and directory services and many more unique identifiers and trusted-third-party network devices are possible.

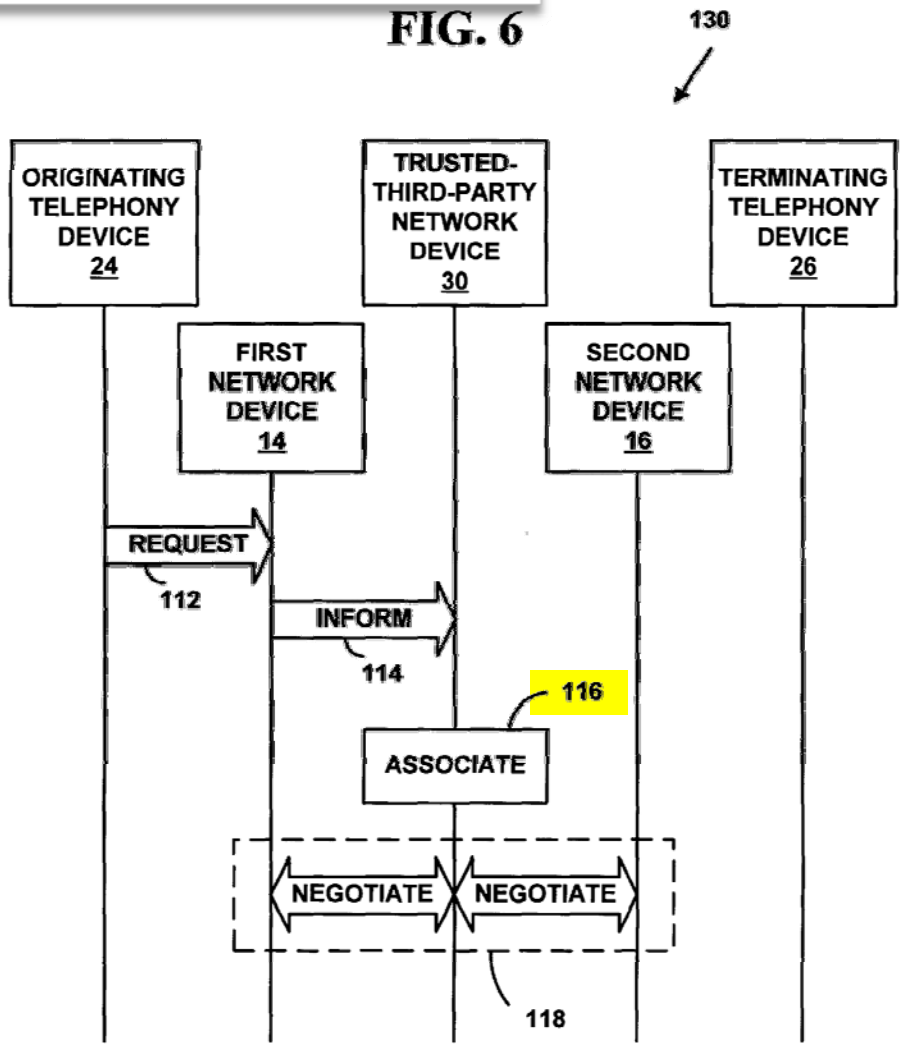
Beser (Ex. 1007) at 11:23-58; Pet. (810) at 33

Grounds Based on Beser and RFC 2401

"a request to look up an Internet Protocol (IP) address"



Beser (Ex. 1007) at Fig. 5; Reply (810) at 10



Beser (Ex. 1007) at Fig. 6; Pet. (810) at 17-19, 34

A public IP **58** address for a second network device **16** is associated with the unique identifier for the terminating telephony device **26** at Step **116**. The second network device **16** is associated with the terminating telephony device **26**. This association of the public IP **58** address for the second network device **16** with the unique identifier is made on the trusted-third-party network device **30**. In one exemplary preferred embodiment, the trusted-third-party network device **30** is a back-end service, a domain name server, or the owner/manager of database or directory services and may be distributed over several physical locations. In another exem-

* * *

For example, the trusted-third-party network device **30** may be a directory service, owned and operated by a telephone company, that retains a list of E.164 numbers of its subscribers. Associated with a E.164 number in the directory database is the IP **58** address of a particular second network device **16**. The database entry may also include a public IP **58** addresses for the terminating telephony device **26**. Many data structures that are known to those skilled in the art are possible for the association of the unique identifiers and IP **58** addresses for the second network devices **16**. However, it should be understood that the present invention is not restricted to E.164 telephone numbers and directory services and many more unique identifiers and trusted-third-party network devices are possible.

Beser (Ex. 1007) at 11:23-58; Pet. (810) at 33

Beser and RFC 2401

"a request to look up an Internet Protocol (IP) address"

UNITED STATES PATENT AND TRADEMAR

BEFORE THE PATENT TRIAL AND APPEAL

APPLE INC.
Petitioner,

v.

VIRNETX, INC. AND SCIENCE APPLICATION IN
CORPORATION,
Patent Owner.

Patent No. 8,868,705
Issued: October 21, 2014
Filed: September 13, 2012
Inventors: Victor Larson, *et al.*
Title: AGILE NETWORK PROTOCOL FOR SECURE
USING SECURE DOMAIN NAMES

Inter Partes Review No. IPR2015-00810

Petition for *Inter Partes* Review of
U.S. Patent No. 8,868,705

310. When the trusted-third-party network device receives a request to initiate a tunneling association, it uses the unique identifier in the request to look-up the corresponding IP address in its database of registered unique identifiers. Ex. 1007 (Beser) at 11:26-36, 11:45-55. To initiate the secure IP tunnel, the trusted-third-party network device will look-up the IP address of the corresponding second network device. Ex. 1007 (Beser) at 9:6-8, 11:26-36.

Ex. 1005 at ¶ 310; Pet. (810) at 34

’705 Patent, Claim 1

1. A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

’705 Patent (Ex. 1001) at Claim 1

address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

to user computer 2601. Thereafter, DNS proxy **2610** returns to user computer **2601** the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) **2604**, preferably using a secure administrative VPN. The address that is returned need not be the actual address of the destination computer.

’705 Patent (Ex. 1001) at 40:18-19

Patent Owner Assertion

"a request to look up an Internet Protocol (IP) address"

Case No. IPR2015-00810

Paper No.

Filed on behalf of: Vir

By:

Joseph E. Palys
Paul Hastings LLP
875 15th Street NW
Washington, DC 2000
Telephone: (202) 551-
Facsimile: (202) 551-
E-mail: josephpalys@

UNITED ST

BEFORE T

Patent Owner

Case IPR2015-00810
Patent 8,868,705

Patent Owner's Response

For example, the Petition alleges that the trusted-third-party network device in *Beser* will "look up and return to the first network device" a "private IP address for the terminating device." (Pet. at 34.) This is incorrect. The first and second network devices, not the trusted-third-party network device, "negotiate" private IP addresses, including the private IP address for the terminating device. (Ex. 1007 at

Opposition at 22

Grounds Based on Beser and RFC 2401

"a request to look up an Internet Protocol (IP) address"

In one exemplary preferred embodiment, the negotiation is carried out through the trusted-third-party network device,

Beser (Ex. 1007) at 9:29-30; Pet. 20, 35-36

US006064968

(12) **United States Patent**
Beser et al.

(10) **Patent No.:**
(45) **Date of Patent:**

(54) **SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS**

(75) Inventors: **Nurettin B. Beser**, Evanston, IL (US); **Michael Borella**, Naperville, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/384,120**

(22) Filed: **Aug. 27, 1999**

(51) **Int. Cl.**[7] **G06F 15/16**; G06F 15/173
(52) **U.S. Cl.** **709/245**; 709/227; 709/225
(58) **Field of Search** 709/220, 222, 709/225, 226, 227, 228, 229, 245, 218, 217; 370/401, 349; 713/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,159,592 A 10/1992 Perkins
5,227,778 A 7/1993 Vacon et al.
5,550,984 A 8/1996 Gelb
5,636,216 A 6/1997 Fox et al.
5,708,655 A 1/1998 Toth et al.
5,793,763 A 8/1998 Mayes et al.
5,812,819 A 9/1998 Rodwin et al.
5,867,660 A 2/1999 Schmidt et al.
5,872,847 A 2/1999 Boyle et al.
6,018,767 A * 1/2000 Fijolek et al. 709/218
6,236,652 B1 * 5/2001 Preston et al. 370/349
6,253,327 B1 * 6/2001 Zhang et al. 713/201
6,377,982 B1 * 4/2002 Rai et al. 709/217

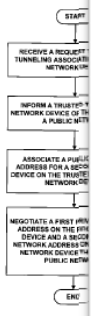
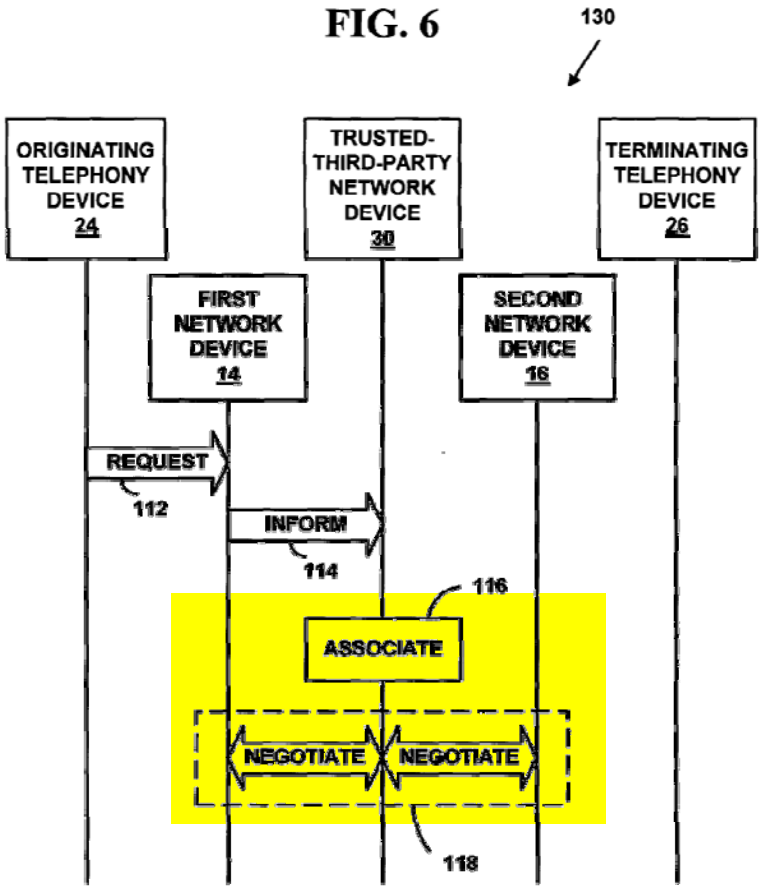


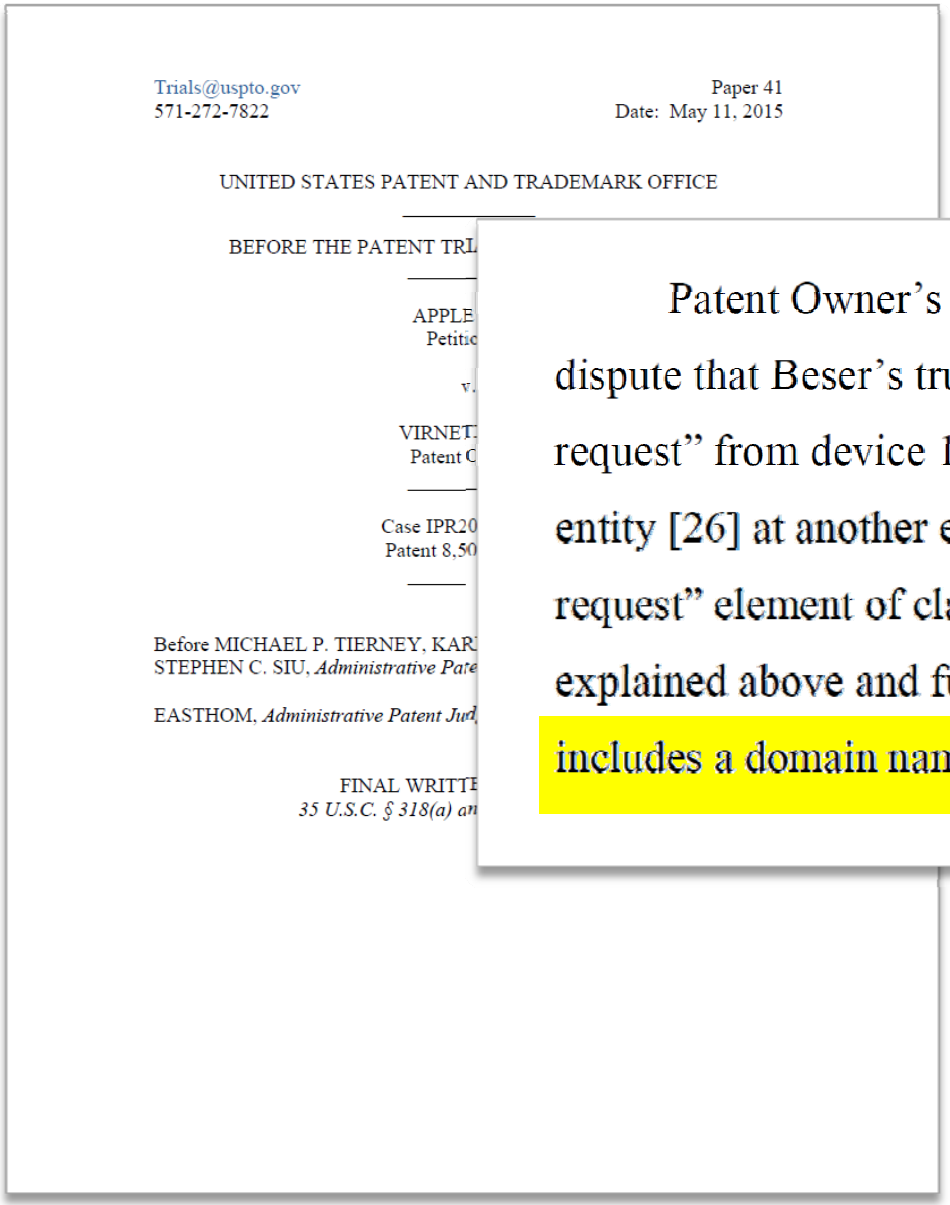
FIG. 6



Beser (Ex. 1007) at Fig. 6; Pet. (810) at 17-18

Final Written Decision in IPR2014-00237

"a request to look up an Internet Protocol (IP) address"



Trials@uspto.gov
571-272-7822

Paper 41
Date: May 11, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRI

APPLE
Petitic

v.

VIRNET
Patent C

Case IPR20
Patent 8,50

Before MICHAEL P. TIERNEY, KAR
STEPHEN C. SIU, *Administrative Pate*

EASTHOM, *Administrative Patent Jud*

FINAL WRITTE
35 U.S.C. § 318(a) an

Patent Owner's characterization of Beser reveals that there is no dispute that Beser's trusted-third-party device 30 is "informed of the request" from device 14; thereby "receiving a request pertaining to a first entity [26] at another entity [14 or 30]" and satisfying the "intercepting a request" element of claim 1 (and a similar element in claim 16). As explained above and further below, Beser's tunneling request, which includes a domain name, is a request for a look up of an IP address. As also

Final Written Decision, IPR2014-00237 at 24; Reply (810) at 8

IPR2015-00810, -812

Ground 1: Beser and RFC 2401

1. Beser and RFC 2401 Issues (810 & 812)

A. Combining Beser and RFC 2401 would have been obvious to one of ordinary skill in the art *(810 claims 1, 21) (812 claims 1, 14)*

B. Beser and RFC 2401 teach "*a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device" (810 claims 1, 21)* (812 claims 1, 14)

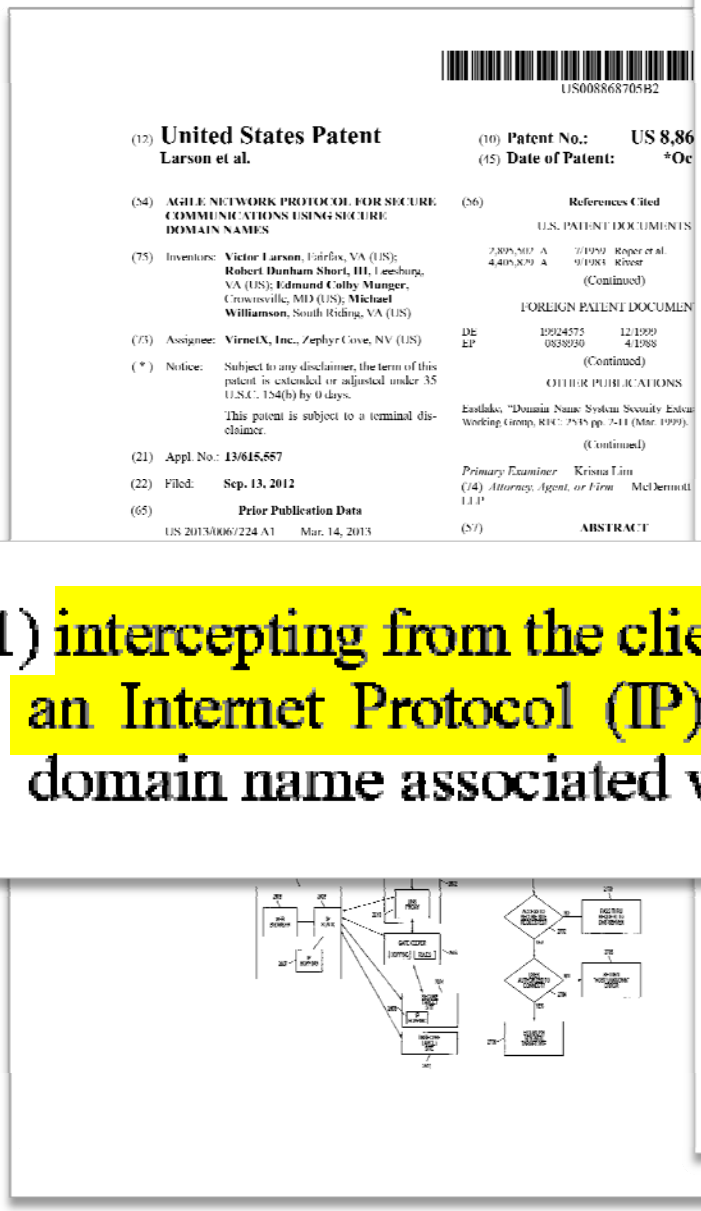
C. Beser and RFC 2401 teach "*intercepting from the client device [the] request to look up an Internet Protocol (IP) address" (810 claims 1, 21) (812 claims 1, 14)*

2. Beser and RFC 2401 Issues (812 only)

A. Beser and RFC 2401 teach *"Receiv[ing]. . . An Indication, a Network Address, and Provisioning Information" (claims 1, 14)*

’705 Patent, Claim 1

“intercepting … [the] request to look up an Internet Protocol (IP) address”



US008868705B2

(12) **United States Patent**
Larson et al.

(10) **Patent No.: US 8,86**
(45) **Date of Patent: *Oc**

(54) **AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmund Colby Munger**, Crownsville, MD (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **VirnetX, Inc.**, Zephyr Cove, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/615,557**

(22) Filed: **Sep. 13, 2012**

(65) **Prior Publication Data**

US 2013/0067224 A1 Mar. 14, 2013

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,305,537 A 7/1999 Roper et al.
4,405,829 A 9/1983 Rivest
(Continued)

FOREIGN PATENT DOCUMEN

DE 19924575 12/1999
EP 0838930 4/1998
(Continued)

OTHER PUBLICATIONS

Eastlake, "Domain Name System Security Exten
Working Group, RFC 2535 pp. 7-11 (Mar. 1999).
(Continued)

Primary Examiner Krisna Lim
(74) *Attorney, Agent, or Firm* McDermott
LLP

(57) **ABSTRACT**

1. A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the

hat the request
responds to a
ications chan-
oviding provi-
he creation of
tween the cli-
ent device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel.

’705 Patent (Ex. 1001) at Claim 1

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

Grounds Based on Beser and RFC 2401

"intercepting … [the] request to look up an Internet Protocol (IP) address"

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

v.

VIRNETX, INC. AND SCIENCE APPLICATION INTERNATIONAL CORPORATION,
Patent Owner.

Patent No. 8,868,705
Issued: October 21, 2014
Filed: September 13, 2012
Inventors: Victor Larson, *et al.*
Title: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Inter Partes Review No. IPR2015-00810

Petition for *Inter Partes* Review of U.S. Patent No. 8,868,705

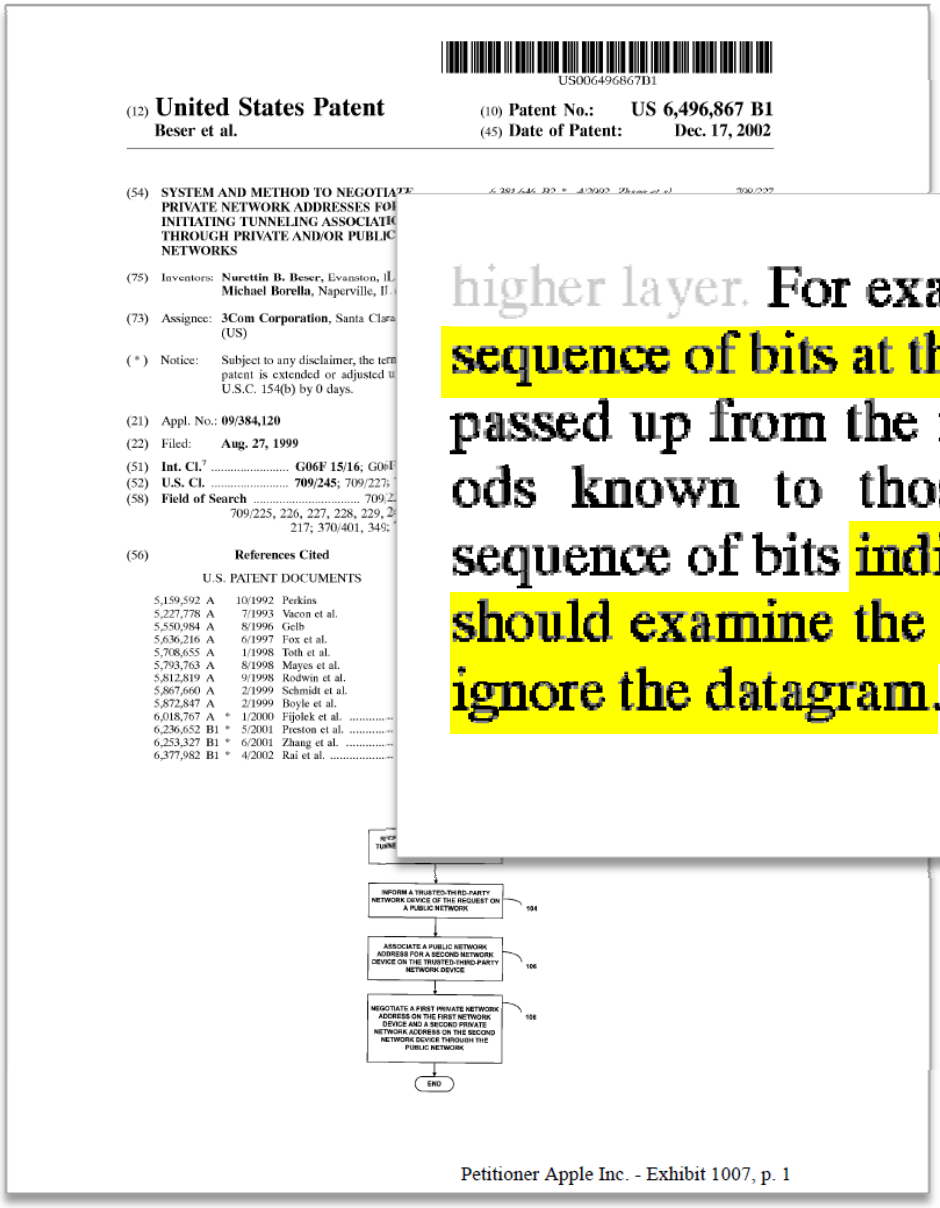
device. Beser shows the first step for initiating an IP tunnel is for an originating end device ("*client device*") to send a request to initiate a tunneling association with a terminating end device ("*target device*"). Ex. 1007 at 7:64-8:1, 9:64-10:41; Ex. 1005 at ¶ 316. The request will be received not by the terminating end device, but by a first network device, which evaluates all of the data packets it receives (*i.e.*, the request is "intercepted" by the first network device). Ex. 1007 at 8:21-47; Ex. 1005 at ¶¶ 299-300, 317, 322. If the first network device determines that a data packet contains a request to initiate an IP tunnel (*e.g.*, due to the presence in it of a distinctive sequence of bits in the datagram), it will forward the packet to the trusted-third-party network device for special processing. Ex. 1007 at 8:21-47; Ex. 1005 at ¶ 322. Otherwise, it processes the packet normally, such as by sending it to a conventional DNS server. Ex. 1007 at 4:7-42, 8:39-44; Ex. 1005 at ¶ 300.

After the trusted-third-party network device receives ("*intercepts*") the request containing the domain name (the unique identifier), it looks up the IP address associated with the domain name. Ex. 1007 at 4:8-11, 8:4-7, 10:38-41,

Pet. at 32-33

Grounds Based on Beser and RFC 2401

"intercepting … [the] request to look up an Internet Protocol (IP) address"



US006496867B1

(12) **United States Patent**
Beser et al.

(10) **Patent No.: US 6,496,867 B1**
(45) **Date of Patent: Dec. 17, 2002**

(54) **SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATION THROUGH PRIVATE AND/OR PUBLIC NETWORKS**

(75) Inventors: **Nurettin B. Beser**, Evanston, IL; **Michael Borella**, Naperville, IL

(73) Assignee: **3Com Corporation**, Santa Clara (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/384,120**

(22) Filed: **Aug. 27, 1999**

(51) **Int. Cl.**[7] **G06F 15/16**; G06F

(52) **U.S. Cl.** **709/245**; 709/227;

(58) **Field of Search** 709/2
709/225, 226, 227, 228, 229, 2
217; 370/401, 349;

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,159,592	A		10/1992	Perkins
5,227,778	A		7/1993	Vacon et al.
5,550,984	A		8/1996	Gelb
5,636,216	A		6/1997	Fox et al.
5,708,655	A		1/1998	Toth et al.
5,793,763	A		8/1998	Mayes et al.
5,812,819	A		9/1998	Rodwin et al.
5,867,660	A		2/1999	Schmidt et al.
5,872,847	A		2/1999	Boyle et al.
6,018,767	A	*	1/2000	Fijolek et al.
6,236,652	B1	*	5/2001	Preston et al.
6,253,327	B1	*	6/2001	Zhang et al.
6,377,982	B1	*	4/2002	Rai et al.

Petitioner Apple Inc. - Exhibit 1007, p. 1

higher layer. For example, the indicator may be a distinctive sequence of bits at the beginning of a datagram that has been passed up from the network and transport layers. By methods known to those skilled in the art, the distinctive sequence of bits indicates to the tunneling application that it should examine the request message for its content and not ignore the datagram. However, the higher layer may be other

Beser (Ex. 1007) at 8:38-43; Pet. (810) at 18

Patent Owner Assertion

"a request to look up an Internet Protocol (IP) address"

Filed on behalf of: VirnetX Inc.
By:
Joseph E. Palys
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-1996
Facsimile: (202) 551-0496
E-mail: josephpalys@paulhastings.com

Naveen Mo
Paul Hastin
875 15th St
Washington
Telephone:
Facsimile:
E-mail: nav

UNITED STATES PATENT AND TRADE

BEFORE THE PATENT TRIAL AND AP

APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2015-00810
Patent 8,868,705

Patent Owner's Response

In *Beser*, when an originating end device wants to communicate with a terminating end device, it sends a tunnel initiation request to the first network device. (Ex. 1007 at 7:65-67; Ex. 2016 at ¶ 37.) Tunneling requests in *Beser* always go to, and are always intended to go to, the first network device. (Ex. 2016 at ¶ 37.) *Beser* does not disclose a single scenario in which a tunneling request is ordinarily received by another entity, but is *instead* received by the first network device. (*Id.*) Nor does *Beser* disclose any scenario in which a tunneling request is

Opposition (810) at 25

88." (Ex. 1007 at 11:15-20.) Thus, the packet received by trusted-third-party network device 30 is "intended for" and "ordinarily received by" trusted-third-party network device 30 since the destination address of the packet contains the address of the trusted-third-party network device 30. Just as with the first network device, *Beser* does not disclose a single scenario in which a tunneling request is ordinarily received by another entity, but is *instead* received by the trusted-third-party network device. (Ex. 2016 at ¶ 38.) Nor does *Beser* disclose any scenario in

Opposition (810) at 22

Patent Owner Admission

Dr. Monrose: tunneling requests are not addressed to the trusted device

source address field 88." (*Id.* at 11:15-20.) Thus, one of skill would have understood that the packet received by trusted-third-party network device 30 is "intended for" and "ordinarily received by" trusted-third-party network device 30 since the destination address of the packet contains the address of the trusted-third-party network device 30. Just as with the first network device, *Beser* does not disclose a single scenario in which a tunneling request is ordinarily received by another entity, but is *instead* received by the trusted-third-party network device.

Ex. 2016 at ¶ 38; Opposition (810) at 26

UNITED STATE

BEFORE THE P

VIRNET

INTE

Case No. IPR2

Case No. IPR2015-00811

Case No. IPR201

DEPOSITION

Thur

Reported by: Joh

Job No. 103298

Q.... You agree that the originating device does not address the tunneling request to the third-party network device, correct?

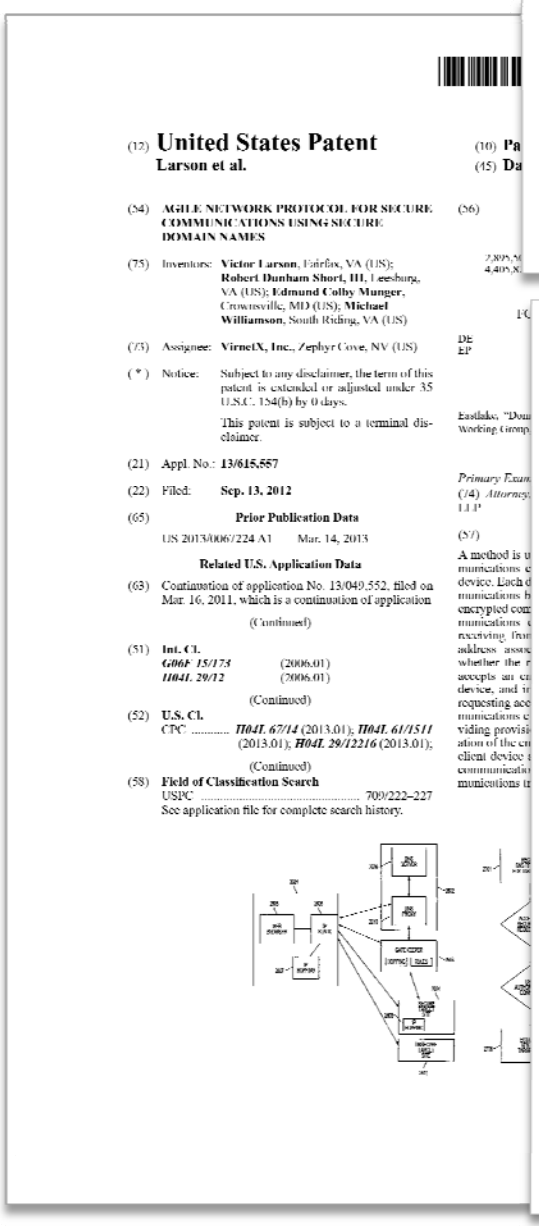
A. Correct.

Ex. 1066 at 101:11-14

Apple v. VirnetX, IPR2015-00810
Petitioner Apple Inc. - Ex. 1066, p. 1

’705 Patent

“intercepting … [the] request to look up an Internet Protocol (IP) address”



(12) **United States Patent**
Larson et al.

(54) **AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmund Colby Munger**, Crownsville, MD (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **VirnetX, Inc.**, Zephyr Cove, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/615,557**

(22) Filed: **Sep. 13, 2012**

(65) **Prior Publication Data**

US 2013/0067224 A1 Mar. 14, 2013

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application

(Continued)

(51) **Int. Cl.**
G06F 15/173 (2006.01)
H04L 29/12 (2006.01)

(Continued)

(52) **U.S. Cl.**
CPC ***H04L 67/14*** (2013.01); ***H04L 61/1511*** (2013.01); ***H04L 29/12216*** (2013.01);

(Continued)

(58) **Field of Classification Search**
USPC 709/222–227
See application file for complete search history.

(56)

(Continued)

(57)

A method is u... munications ... device. Each ... munications ... encrypted com... munications ... receiving, [from] ... address assoc... whether the r... accepts an ca... device, and ir... requesting acc... munications ... viding provisi... ation of the ca... client device ... communicatio... munications ...

According to one embodiment, DNS proxy **2610** intercepts all DNS lookup functions from client **2605** and determines whether access to a secure site has been requested. If access to

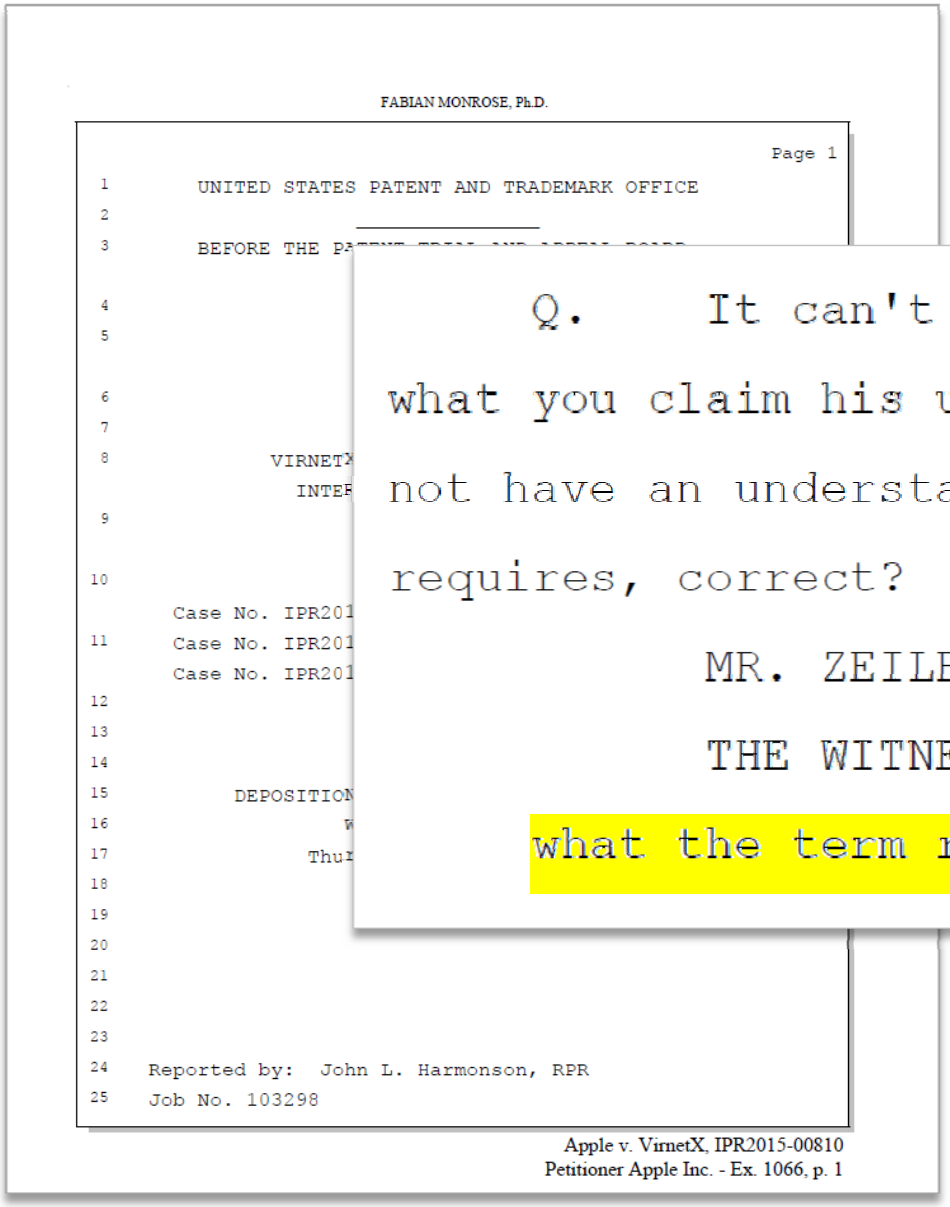
’705 Patent (Ex. 1001) at 40:1-3

which the request was intended. Based on my review of the specification, the most germane discussion in the patent of this concept relates to a DNS proxy that “intercepts” all DNS lookup functions in order to determine whether access to a secure site has been requested. Ex. 1001 (705 patent) at 40:1-7, Figs. 26 & 27. The specification explains that while the DNS server (2609) ordinarily would receive and resolve domain name requests, DNS requests are instead routed to the DNS proxy. Ex. 1001 (705 patent) at 40:1-3. The patents indicate the DNS proxy and DNS server can, in one configuration, be deployed on separate computers. Ex. 1001 (705 patent) at 40:38-42. It is therefore my opinion that the ’705 patent uses the term “intercept” to mean receipt of a message by a DNS proxy server instead of the intended destination (the DNS server).

Ex. 1005 at ¶ 68; Pet. (810) at 10

Patent Owner Admission

Dr. Monrose: has no opinion about what "*intercepting*" requires



FABIAN MONROSE, Ph.D.

Page 1

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PA

VIRNETX
INTER

Case No. IPR201
Case No. IPR201
Case No. IPR201

DEPOSITION
W
Thur

Reported by: John L. Harmonson, RPR
Job No. 103298

Apple v. VirnetX, IPR2015-00810
Petitioner Apple Inc. - Ex. 1066, p. 1

Q. It can't perform intercepting under what you claim his understanding is. But you do not have an understanding of what the term requires, correct?

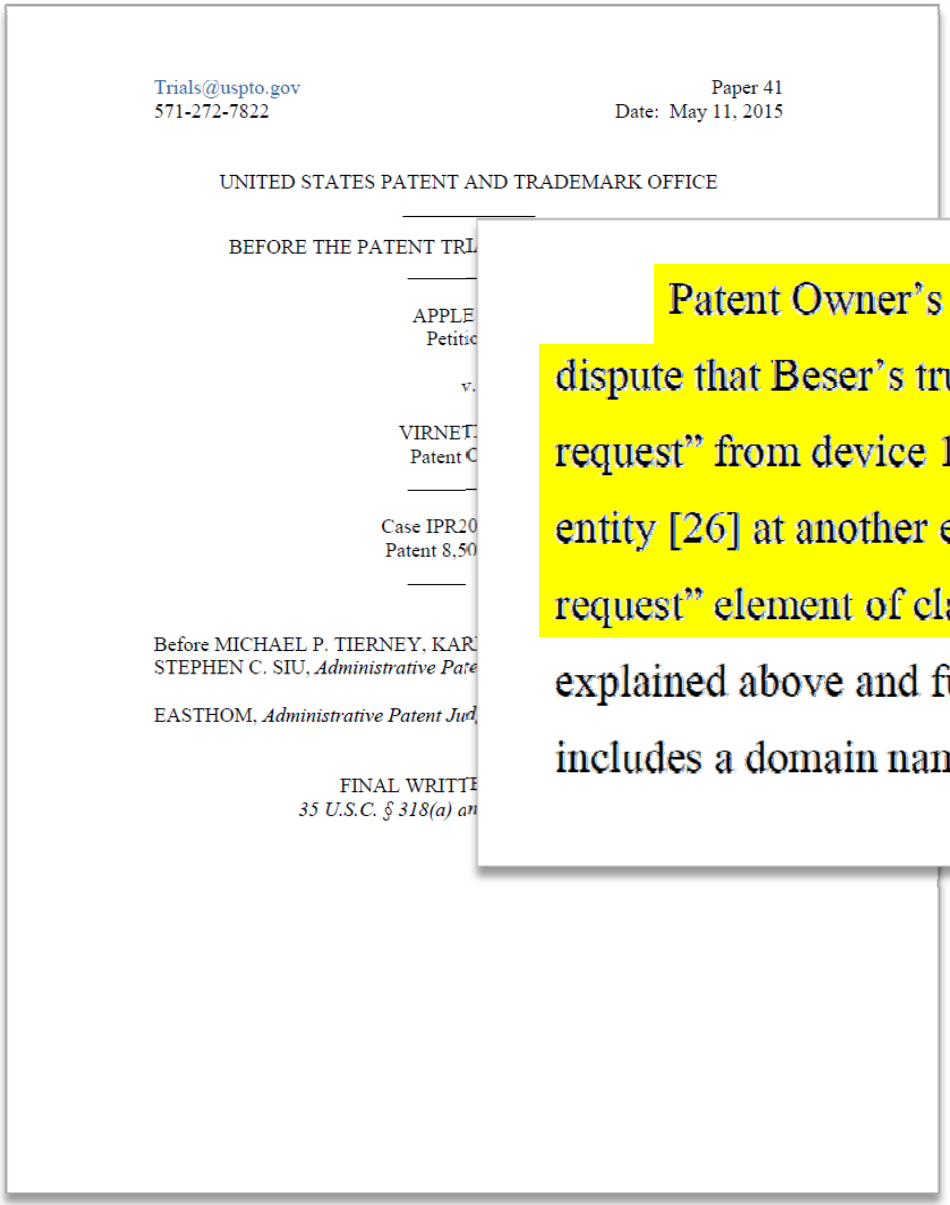
MR. ZEILBERGER: Objection; form.

THE WITNESS: I made no opinion of what the term requires.

Ex. 1066 at 132:7-13; Reply (810) at 14

Final Written Decision in IPR2014-00237

"intercepting … [the] request to look up an Internet Protocol (IP) address"



Trials@uspto.gov
571-272-7822

Paper 41
Date: May 11, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRI

APPLE
Petitic

v.

VIRNET
Patent C

Case IPR20
Patent 8,50

Before MICHAEL P. TIERNEY, KAR
STEPHEN C. SIU, *Administrative Pate*

EASTHOM, *Administrative Patent Jud*

FINAL WRITTE
35 U.S.C. § 318(a) an

Patent Owner's characterization of Beser reveals that there is no dispute that Beser's trusted-third-party device 30 is "informed of the request" from device 14; thereby "receiving a request pertaining to a first entity [26] at another entity [14 or 30]" and satisfying the "intercepting a request" element of claim 1 (and a similar element in claim 16). As explained above and further below, Beser's tunneling request, which includes a domain name, is a request for a look up of an IP address. As also

Final Written Decision, IPR2014-00237 at 24; Reply (810) at 8

IPR2015-00810, -812

1. **Beser and RFC 2401 Issues (810 & 812)**

   A. Combining Beser and RFC 2401 would have been obvious to one of ordinary skill in the art *(810 claims 1, 21) (812 claims 1, 14)*

   B. Beser and RFC 2401 teach "*a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device" (810 claims 1, 21)* (812 claims 1, 14)

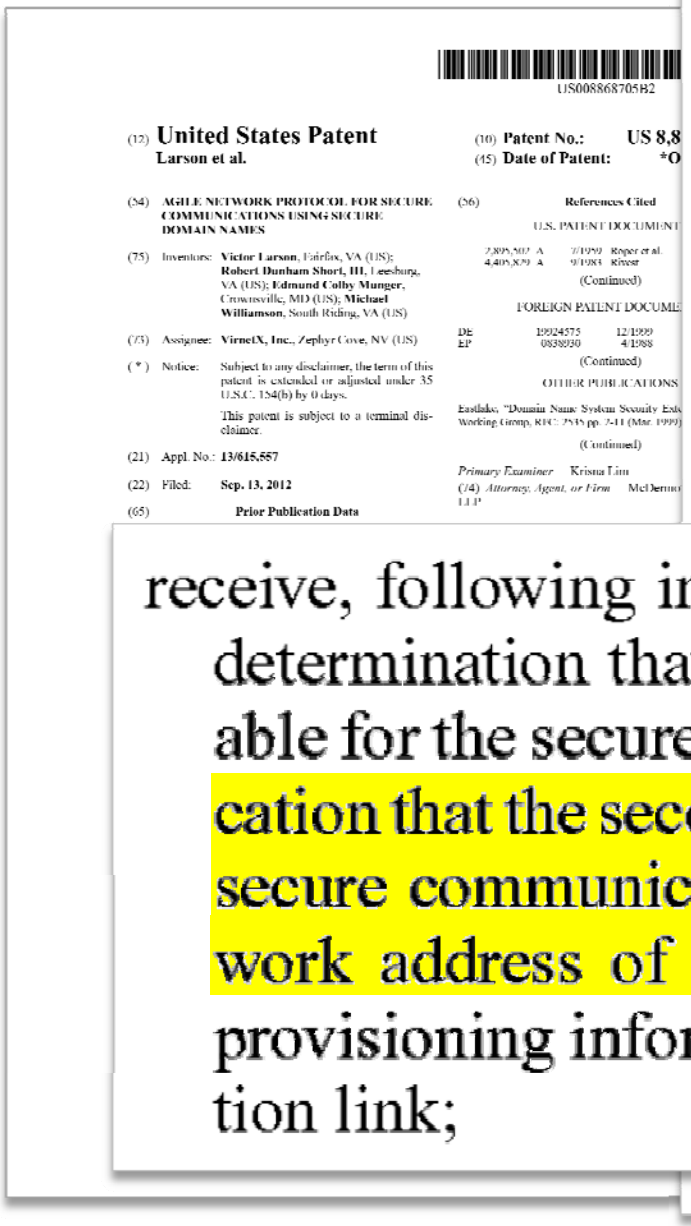
   C. Beser and RFC 2401 teach "*intercepting from the client device [the] request to look up an Internet Protocol (IP) address" (810 claims 1, 21) (812 claims 1, 14)*

2. **Beser and RFC 2401 Issues (812 only)**

   A. Beser and RFC 2401 teach *"Receiv[ing]. . . An Indication, a Network Address, and Provisioning Information" (claims 1, 14)*

’009 Patent, Claim 1

“*receive*” an “*indication*” and the “*network address*”



US008868705B2

(12) **United States Patent**
Larson et al.

(10) **Patent No.: US 8,8**
(45) **Date of Patent: *O**

(54) **AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmund Colby Munger**, Crownsville, MD (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **VirnetX, Inc.**, Zephyr Cove, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/615,557**

(22) Filed: **Sep. 13, 2012**

(65) **Prior Publication Data**

(56) **References Cited**

U.S. PATENT DOCUMENT

7,305,502 A 7/1999 Roper et al.
4,405,829 A 9/1983 Rivest
(Continued)

FOREIGN PATENT DOCUME

DE 19924575 12/1999
EP 0838930 4/1988
(Continued)

OTHER PUBLICATIONS

Eastlake, "Domain Name System Security Exte
Working Group, RFC 2535 pp. 7-11 (Mar. 1999)
(Continued)

Primary Examiner Krista Lin
(74) *Attorney, Agent, or Firm* McDermo
LLP

1. A network device, comprising:

a storage device storing an application program for a secure communications service; and

at least one processor configured to execute the application program for the secure communications service so as to enable the network device to:

send a domain name service (DNS) request to look up a network address of a second network device based on an identifier associated with the second network device;

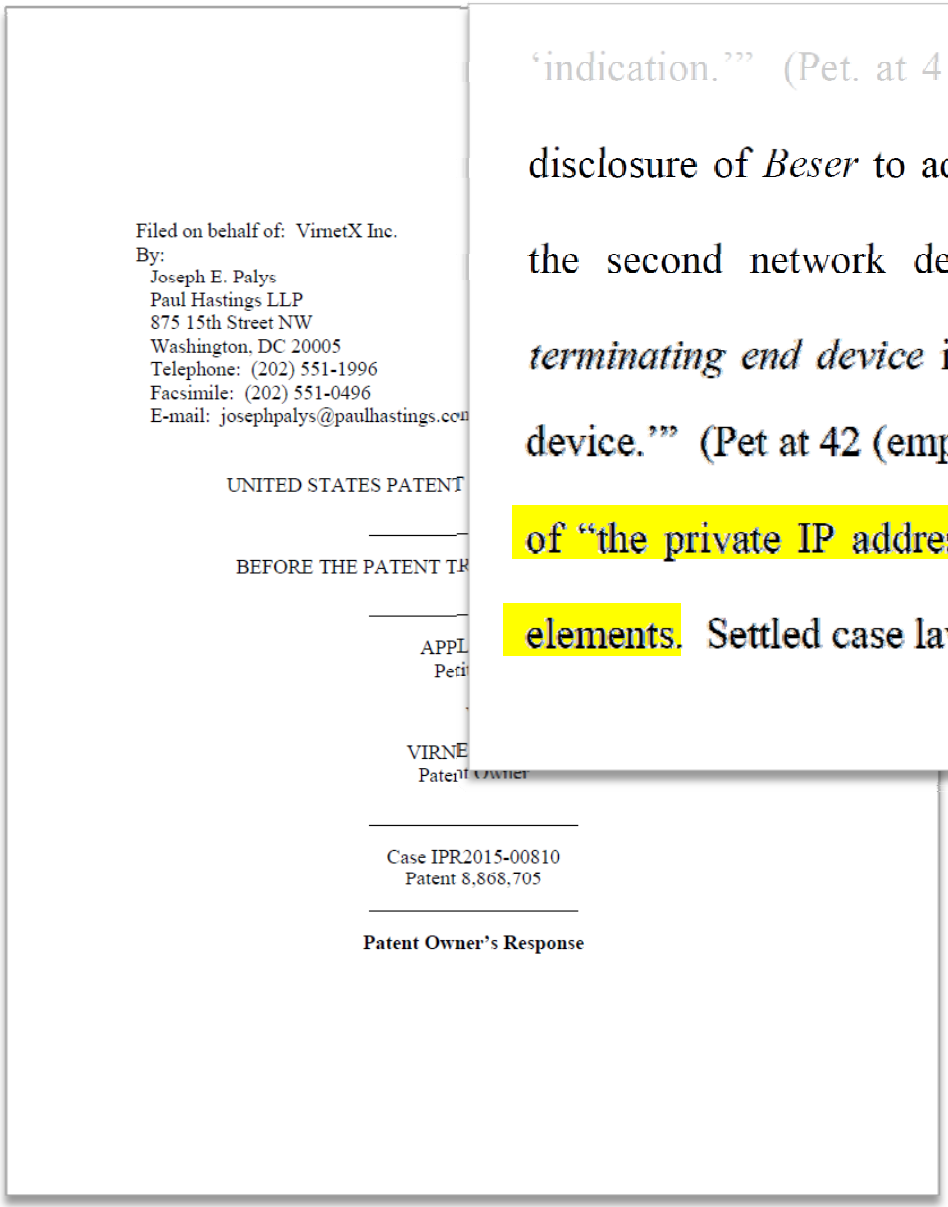
receive, following interception of the DNS request and a determination that the second network device is available for the secure communications service: (1) an indication that the second network device is available for the

receive, following interception of the DNS request and a determination that the second network device is available for the secure communications service: (1) an indication that the second network device is available for the secure communications service, (2) the requested network address of the second network device, and (3) provisioning information for an encrypted communication link;

’009 Patent (Ex. 1001) at Claim 1

Patent Owner Assertion

Beser does not show both "*an indication*" and a "*network address*"



Filed on behalf of: VirnetX Inc.
By:
Joseph E. Palys
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-1996
Facsimile: (202) 551-0496
E-mail: josephpalys@paulhastings.com

UNITED STATES PATENT

BEFORE THE PATENT TR

APPL
Peti

VIRNE
Paten

Case IPR2015-00810
Patent 8,868,705

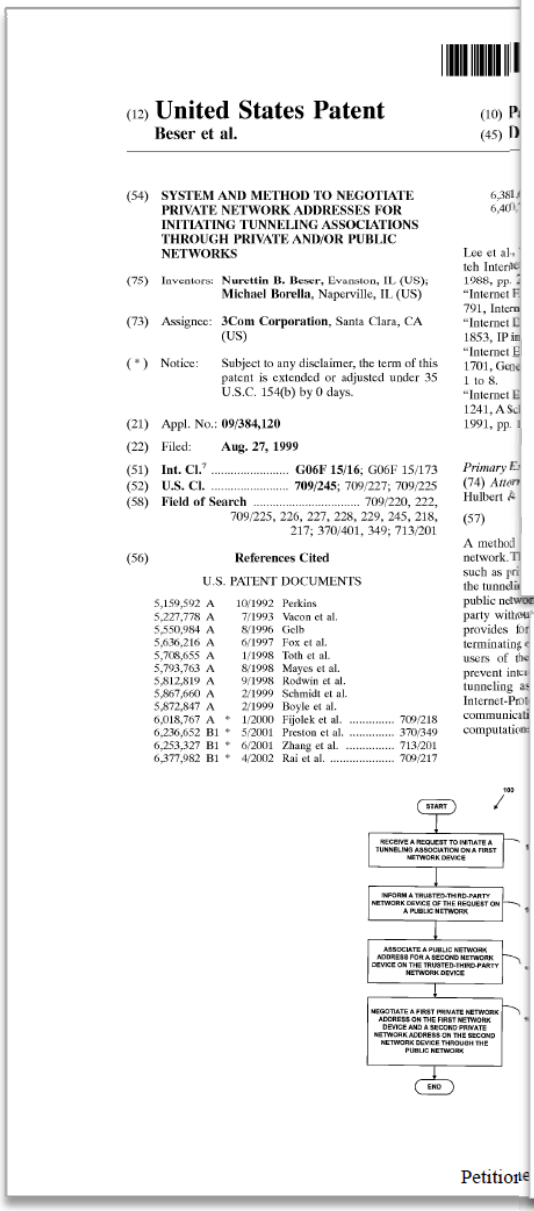
Patent Owner's Response

'indication.'" (Pet. at 41 (emphasis added).) Petitioner relies on an overlapping disclosure of *Beser* to address the claimed "(2) the requested network address of the second network device," arguing that "[t]he *private IP address of the terminating end device* is 'the requested network address of the second network device.'" (Pet at 42 (emphasis added).) In other words, Petitioner relies on receipt of "the private IP address of the terminating end device" to address both claim elements. Settled case law reveals the error in Petitioner's analysis.

Response (812) at 40-41

Grounds Based on Beser and RFC 2401

Beser teaches "*an indication*" and a "*network address*"



(12) **United States Patent**
Beser et al.

(10) P
(45) D

(54) **SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS**

(75) Inventors: **Nurettin B. Beser**, Evanston, IL (US); **Michael Borella**, Naperville, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/384,120**

(22) Filed: **Aug. 27, 1999**

(51) **Int. Cl.**[7] **G06F 15/16**; G06F 15/173
(52) **U.S. Cl.** **709/245**; 709/227; 709/225
(58) **Field of Search** 709/220, 222, 709/225, 226, 227, 228, 229, 245, 218, 217; 370/401, 349; 713/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,159,592	A	10/1992	Perkins	
5,227,778	A	7/1993	Vacon et al.	
5,550,984	A	8/1996	Gelb	
5,636,216	A	6/1997	Fox et al.	
5,708,655	A	1/1998	Toth et al.	
5,793,763	A	8/1998	Mayes et al.	
5,812,819	A	9/1998	Rodwin et al.	
5,867,660	A	2/1999	Schmidt et al.	
5,872,847	A	2/1999	Boyle et al.	
6,018,767	A *	1/2000	Fijolek et al.	709/218
6,236,652	B1 *	5/2001	Preston et al.	370/349
6,253,327	B1 *	6/2001	Zhang et al.	713/201
6,377,982	B1 *	4/2002	Rai et al.	709/217

Petitione

and the terminating end of the tunneling association." Ex. 1007 at 8:15-18. By receiving both its own private IP address and the private address of the terminating end device, the originating end device ("*first network device*") receives an "indication" (*i.e.*, something that shows the probable presence or existence or nature of) that an IP tunnel is in operation and the terminating end device is able to communicate via the IP tunnel ("*that the second network device is available for the secure communications service*"). Ex. 1005 at ¶¶ 101, 341. Accordingly, Beser

Pet. (812) at 41

The assignment of private network addresses to the ends of the tunneling association may also include transmitting the private network addresses to the network devices at the ends of the tunneling association where the private network addresses are stored on these end devices. For example, the originating network device **24** may store the private network addresses for the originating and terminating ends of the tunneling association on the originating network device **24**.

Beser (Ex. 1007) at 21:48-54; Pet. (812) at 41; Reply (812) at 17

Grounds

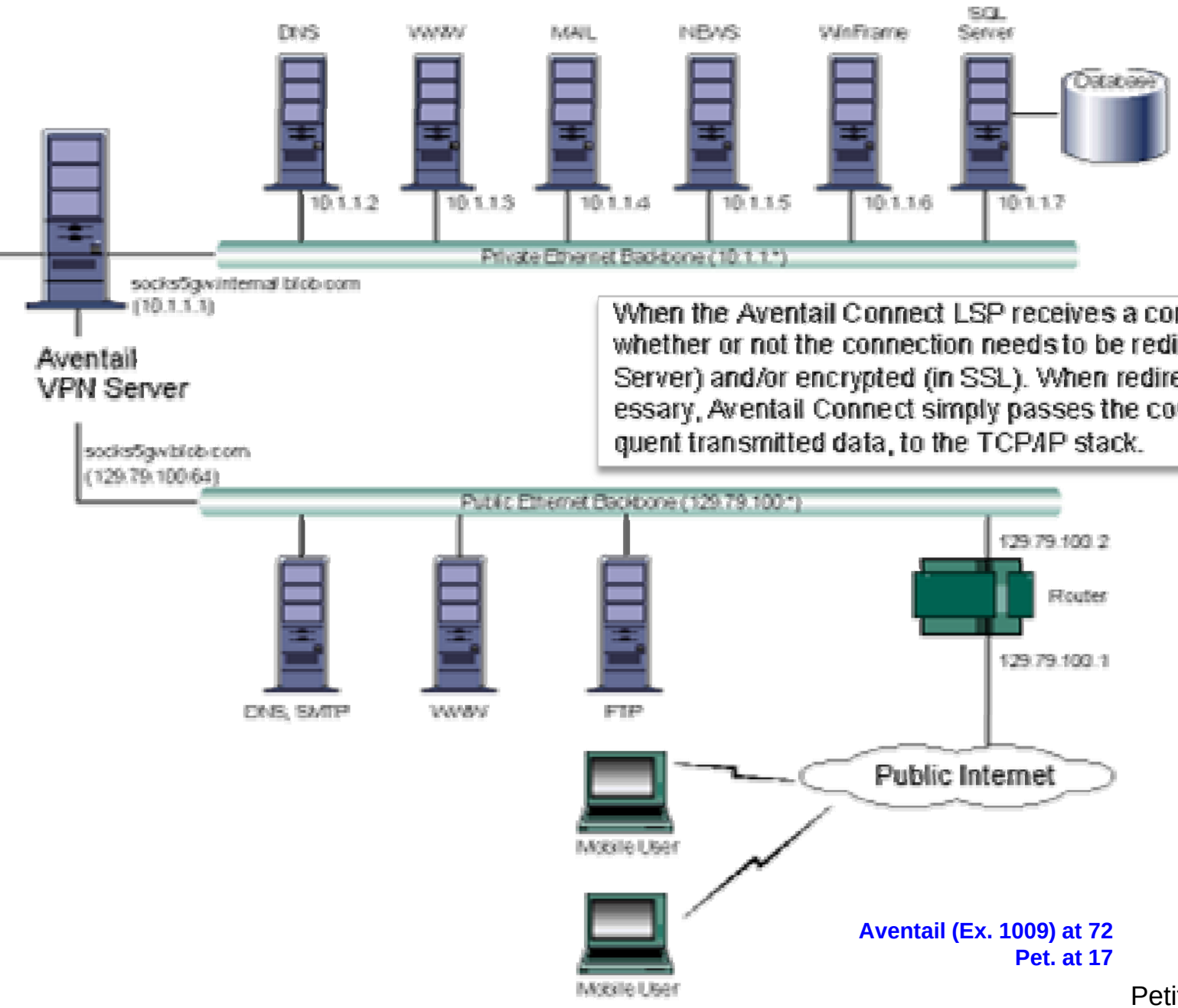
1. **Whether Claims 1-3, 6, 14, 16-25, 28, 31, and 34 are obvious under 35 U.S.C. § 103 over Aventail (Ex. 1009) and RFC 2401 (Ex. 1008)**

2. Whether Claims 8-10, 12, 15, 30 and 32 are obvious under 35 U.S.C. § 103 over Aventail, RFC 2401 and RFC 2543 (Ex. 1013)

3. Whether Claims 4, 5, 7, 26, 27, and 29 are obvious under 35 U.S.C. § 103 over Aventail, RFC 2401 and Brand (Ex. 1012)

4. Whether Claims 11 and 13 are obvious under 35 U.S.C. § 103 over Aventail, RFC 2401, RFC 2543 and Brand

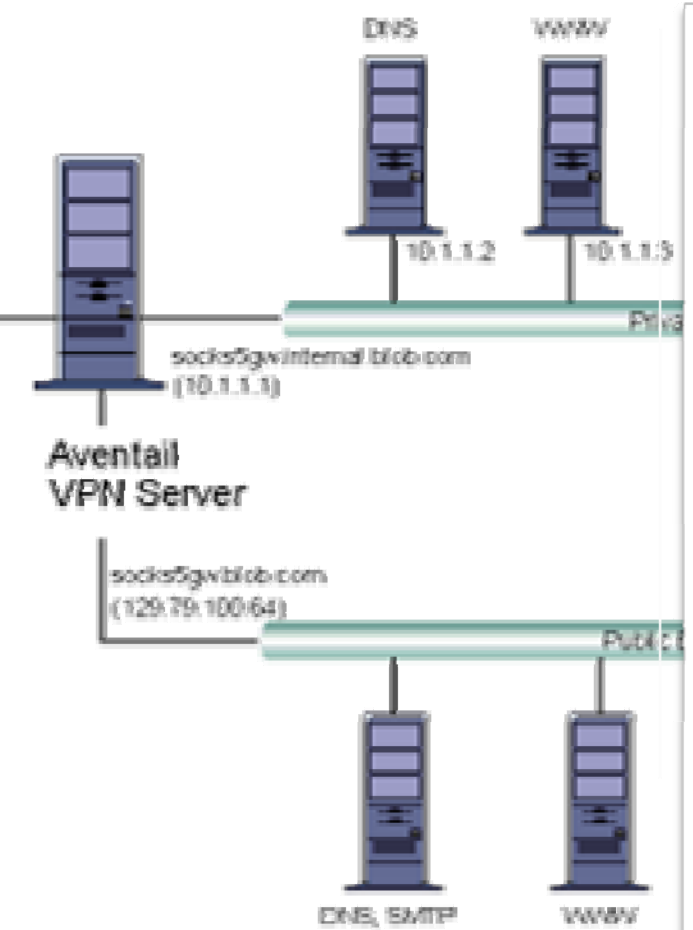
Grounds Based on Aventail and RFC 2401



When the Aventail Connect LSP receives a connection request, it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) and/or encrypted (in SSL). When redirection and encryption are not necessary, Aventail Connect simply passes the connection request, and any subsequent transmitted data, to the TCP/IP stack. **Aventail (Ex. 1009) at 10; Pet. at 19, 33**

Aventail (Ex. 1009) at 72
Pet. at 17

Grounds Based on Aventail and RFC 2401



How Does Aventail Connect Work?

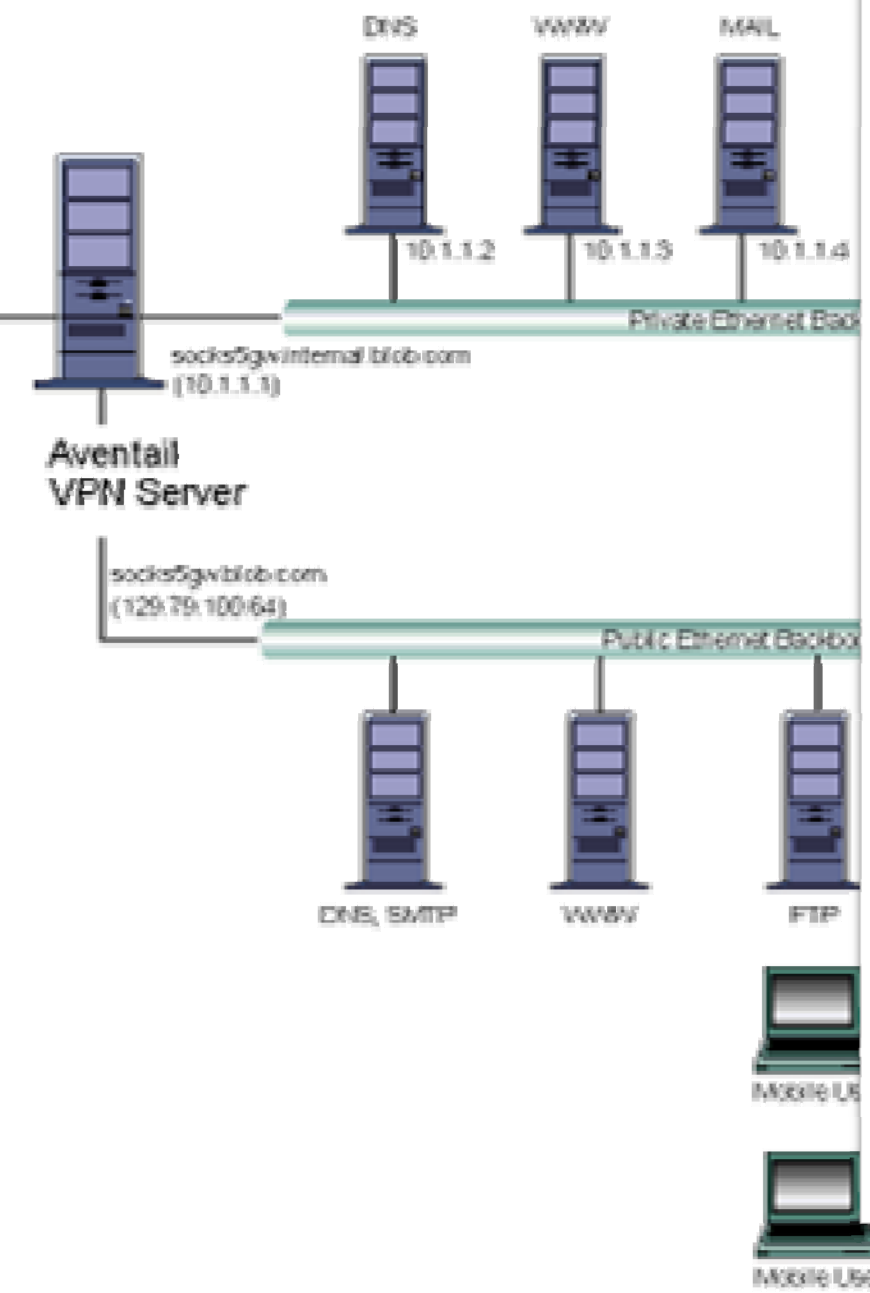
The following three steps are identical to standard WinSock communications steps described above; however, nested inside them are additional actions and options introduced by Aventail Connect.

1. The application does a DNS lookup to convert the hostname to an IP address. If the application already knows the IP address, this entire step is skipped. Otherwise, Aventail Connect does the following:

   - If the hostname matches a local domain string or does not match a redirection rule, Aventail Connect passes the name resolution query through to the TCP/IP stack on the local workstation. The TCP/IP stack performs the lookup as if Aventail Connect were not running.
   - If the destination hostname matches a redirection rule domain name (i.e., the host is part of a domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution.
   - If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a fake DNS entry that it can recognize later, and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied, and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request.

Aventail (Ex. 1009) at 11-12
Pet. at 31-32, *passim*

Grounds Based on Aventail and RFC 2401



2. The application requests a connection to the remote host. This causes the underlying stack to begin the TCP handshake. When the handshake is complete, the application is notified that the connection is established and that data may now be transmitted and received. Aventail Connect does the following:

   a. Aventail Connect checks the connection request.

      - If the request contains a false DNS entry (from step 1), it will be proxied.
      - If the request contains a routable IP address, and the rules in the configuration file say it must be proxied, Aventail Connect will call WinSock to begin the TCP handshake with the server designated in the configuration file.
      - If the request contains a real IP address and the configuration file rule says that it does not need to be proxied, the request will be passed to WinSock and processing jumps to step 3 as if Aventail Connect were not running.

   b. When the connection is completed, Aventail Connect begins the SOCKS negotiation.

      - It sends the list of authentication methods enabled in the configuration file.
      - Once the server selects an authentication method, Aventail Connect executes the specified authentication processing.
      - It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.

   c. When the SOCKS negotiation is completed, Aventail Connect notifies the application. From the application's point of view, the entire SOCKS negotiation, including the authentication negotiation, is merely the TCP handshaking.

Aventail (Ex. 1009) at 11-12
Pet. at 31-32, *passim*

IPR2015-00811

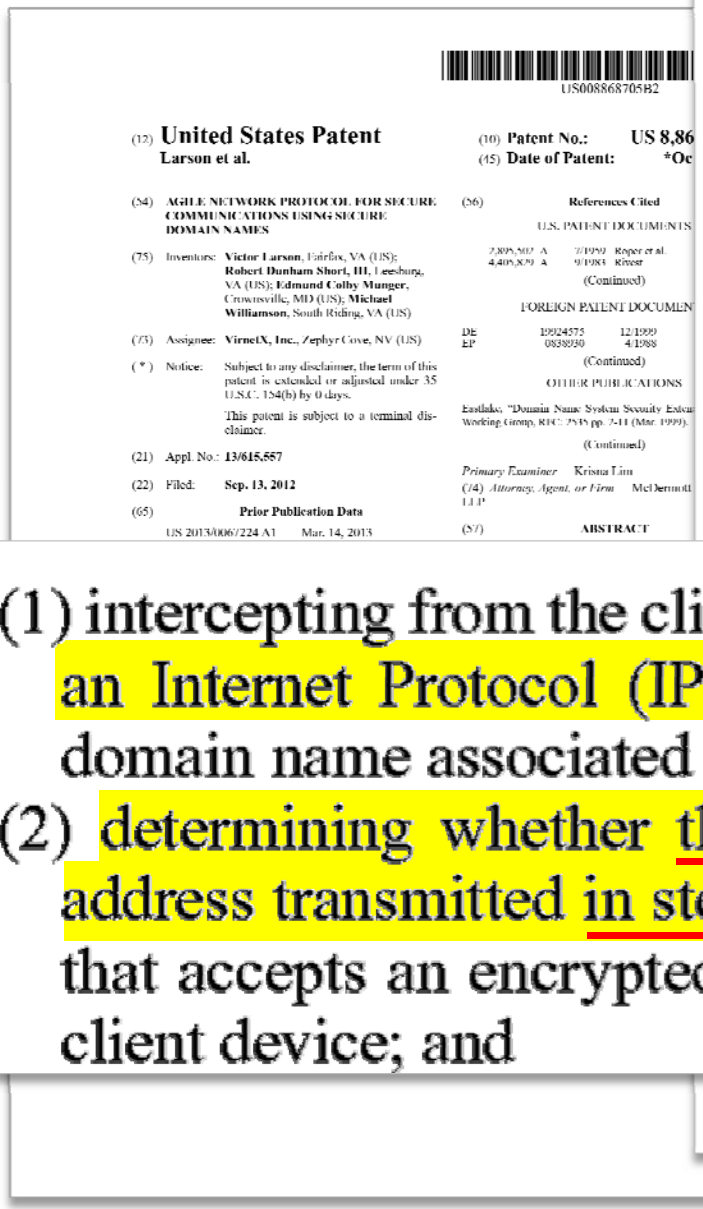
1. Aventail and RFC 2401 Issues

A. Aventail and RFC 2401 teach "*Determining Whether the Request to Look Up the IP Address [Intercepted] in Step (1) . . . Corresponds to a Device that Accepts an Encrypted Channel Connection*" (claims 1, 21)

B. Aventail and RFC 2401 teach "*Encrypted Communications Channel Between the Client Device and the Target Device*" (claims 1, 21)

C. Aventail and RFC 2401 teach *"In Response to Determining . . . Providing Provisioning Information" (claims 1, 21)*

’705 Patent, Claim 1



US008868705B2

(12) **United States Patent**
Larson et al.

(10) **Patent No.: US 8,86**
(45) **Date of Patent: *Oc**

(54) **AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmund Colby Munger**, Crownsville, MD (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **VirnetX, Inc.**, Zephyr Cove, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/615,557**

(22) Filed: **Sep. 13, 2012**

(65) **Prior Publication Data**

US 2013/0067224 A1 Mar. 14, 2013

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,305,537 A 7/1999 Roper et al.
4,405,829 A 9/1983 Rivest
(Continued)

FOREIGN PATENT DOCUMEN

DE 19924575 12/1999
EP 0838930 4/1988
(Continued)

OTHER PUBLICATIONS

Eastlake, "Domain Name System Security Exten
Working Group, RFC 2535 pp. 7-11 (Mar. 1999).
(Continued)

Primary Examiner Krisna Lim
(74) *Attorney, Agent, or Firm* McDermott
LLP

(57) **ABSTRACT**

1. A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the

at the request
responds to a
ications chan-
oviding provi-
he creation of
tween the cli-
the encrypted
data commu-
ices, the client
accesses the

encrypted communications channel.

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

’705 Patent (Ex. 1001) at Claim 1

Grounds Based on Aventail and RFC 2401

"a request to look up an Internet Protocol (IP) address"

Aventail discloses this element in two ways.

Pet. at 31
Reply at 7

Aventail discloses this element in two ways. First, Aventail shows that a client computer running Aventail Connect will transparently intercept each connection request made on the client. Ex. 1009 at 7-9, 72-73; Ex. 1005 ¶¶ 171-172, 209-216. For example, Aventail discloses that to connect to a "Remote Host" ("*target device*"), an application on the client device "executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address." Ex. 1009 at 8; *see also* Ex. 1009 at 11;

Pet. at 31

Inventors: Victor Larson, *et al.*
Title: AGILE NETWORK PROTOCOL FOR SECURE COMMU
USING SECURE DOMAIN NAMES

Inter Partes Review No. IPR2015-00811

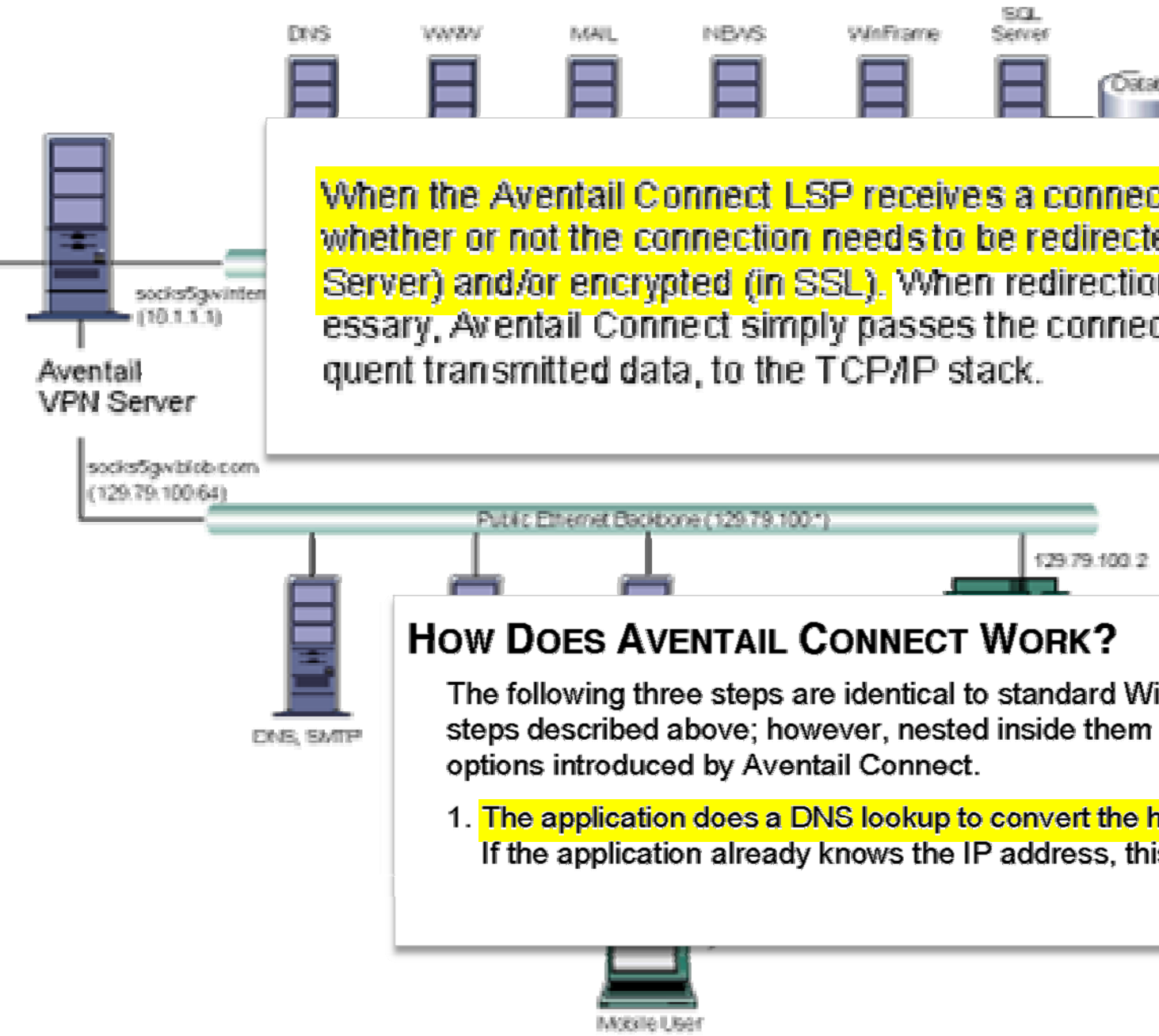
Petition for *Inter Partes* Review of U.S. Patent No. 8,868,705

The first "intercept[ion]" in Aventail follows an application's initial request to connect to a remote host. Pet. at 31-32; Ex. 1009 at 9-11; Ex. 1005 at ¶¶ 209-20. Aventail explains the application on the client device executes "a DNS lookup to convert the hostname" in the request into "an IP address." *Id.* This "domain name conversion request" is "intercepted" by the Aventail Connect software on the client device. Dec. at 15; Ex. 1005 at ¶¶ 219-220.

Reply at 7

Grounds Based on Aventail and RFC 2401

"a request to look up an Internet Protocol (IP) address"



When the Aventail Connect LSP receives a connection request, it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) and/or encrypted (in SSL). When redirection and encryption are not necessary, Aventail Connect simply passes the connection request, and any subsequent transmitted data, to the TCP/IP stack.

Aventail (Ex. 1009) at 10
Pet. at 19, 33

How Does Aventail Connect Work?

The following three steps are identical to standard WinSock communications steps described above; however, nested inside them are additional actions and options introduced by Aventail Connect.

1. The application does a DNS lookup to convert the hostname to an IP address. If the application already knows the IP address, this entire step is skipped.

Aventail (Ex. 1009) at 11-12

Grounds Based on Aventail and RFC 2401

"a request to look up an Internet Protocol (IP) address"

Second, Aventail shows that the Aventail Connect client can be configured to route all connection requests to the Aventail Extranet server for handling and resolution. Ex. 1009 at 61; *see also* Ex. 1009 at 12. The server in this configuration will receive the connection request containing either the IP address or the domain name of the destination computer—from the client computer running Aventail Connect, and resolves these connection requests. Ex. 1009 at 12;

Pet. at 32

Patent Owner.

Patent No. 8,868,705
Issued: October 21, 201
Filed: September 13, 201
Inventors: Victor Larson, *e*
Title: AGILE NETWORK PROTOCOL FOR SEC
USING SECURE DOMAIN N

Inter Partes Review No. IPR201

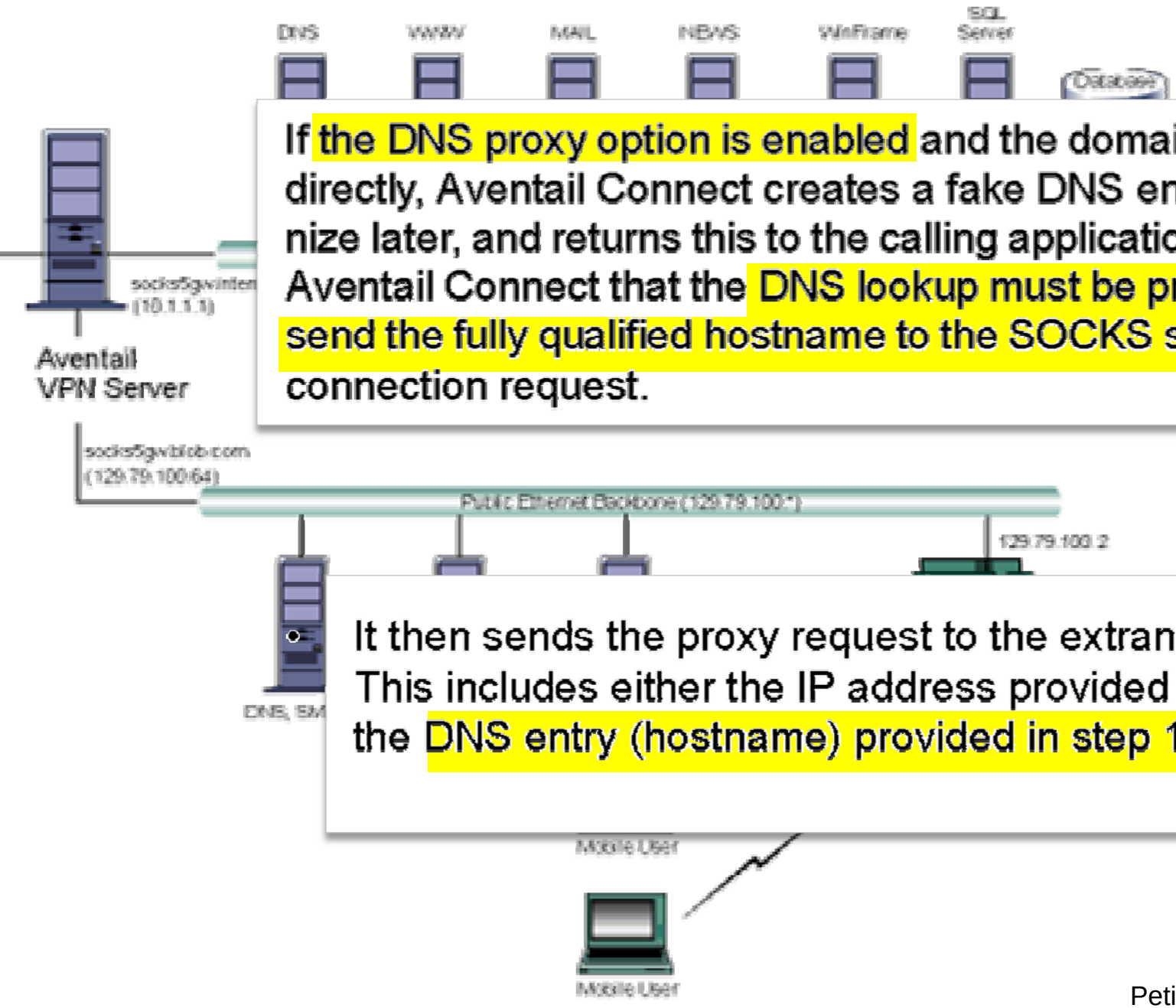
Petition for *Inter Partes* Rev
U.S. Patent No. 8,868,70

Aventail also discloses a second "intercept[ion]," as the Board found, through the technique of proxying that same "request" to the Aventail Extranet Server, which receives the request and resolves the hostname into an IP address. Dec. at 32; Pet at. 32; Ex. 1009 at 12, 61. Patent Owner does not dispute either of

Reply at 7

Grounds Based on Aventail and RFC 2401

"a request to look up an Internet Protocol (IP) address"



If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a fake DNS entry that it can recognize later, and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied, and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request.

Aventail (Ex. 1009) at 11-12
Pet. at 31-32, *passim*

It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.

Aventail (Ex. 1009) at 11-12
Pet. at 31-32, *passim*

Grounds Based on Aventail and RFC 2401

"a request to look up an Internet Protocol (IP) address"

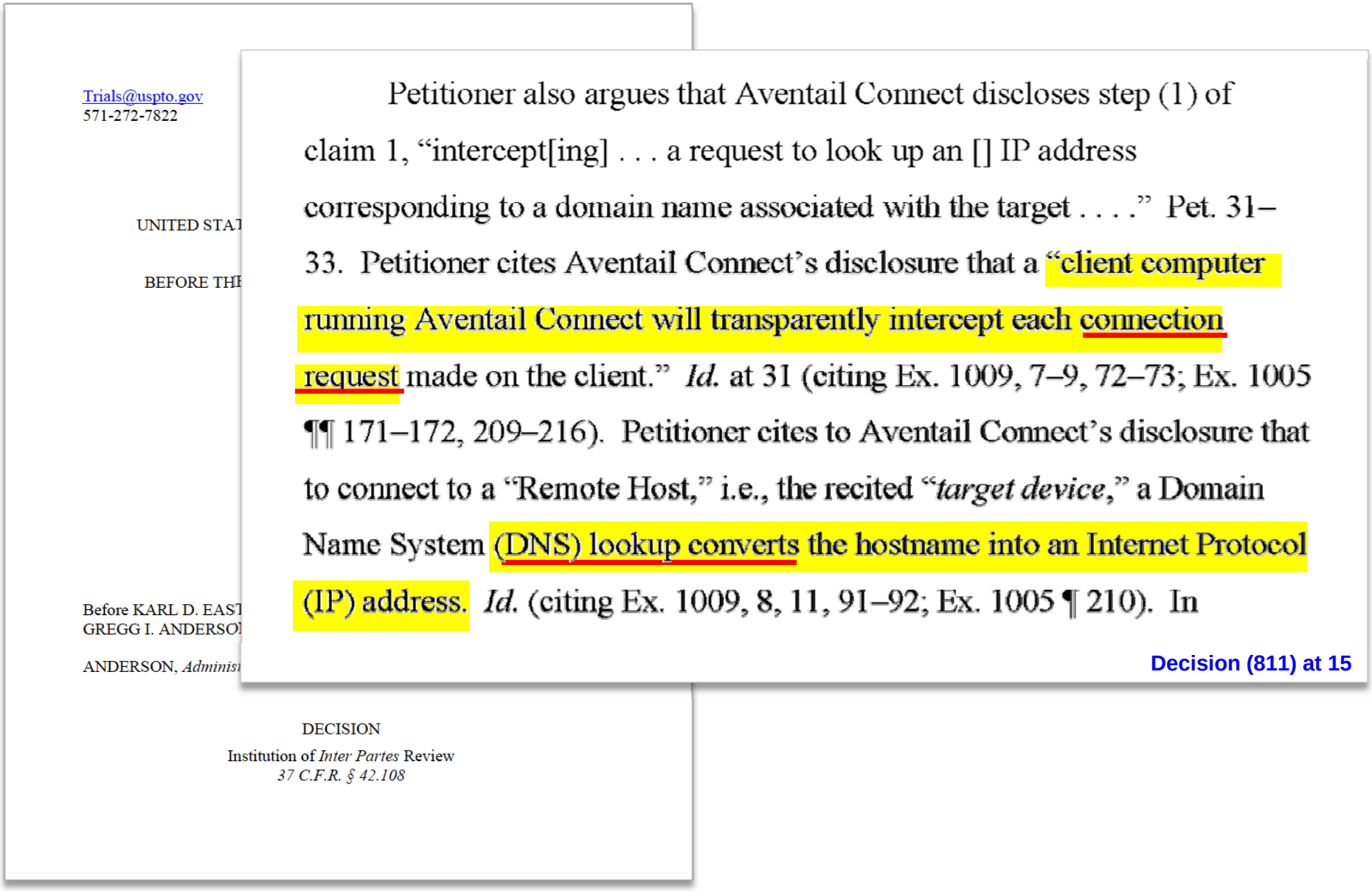
Paper No. 1

In either configuration, Aventail meets the "*interception*" element of the claims because either the client computer running Aventail Connect or the Extranet server receives and acts on the DNS requests – neither is the destination specified in the connection request. *See* Ex. 1001 at 12 ("It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.") Pet. at 33

Petition for *Inter Partes* Review of
U.S. Patent No. 8,868,705

Institution Decision

"a request to look up an Internet Protocol (IP) address"



Trials@uspto.gov
571-272-7822

UNITED STA

BEFORE THE

Before KARL D. EAST
GREGG I. ANDERSO

ANDERSON, *Adminis*

DECISION

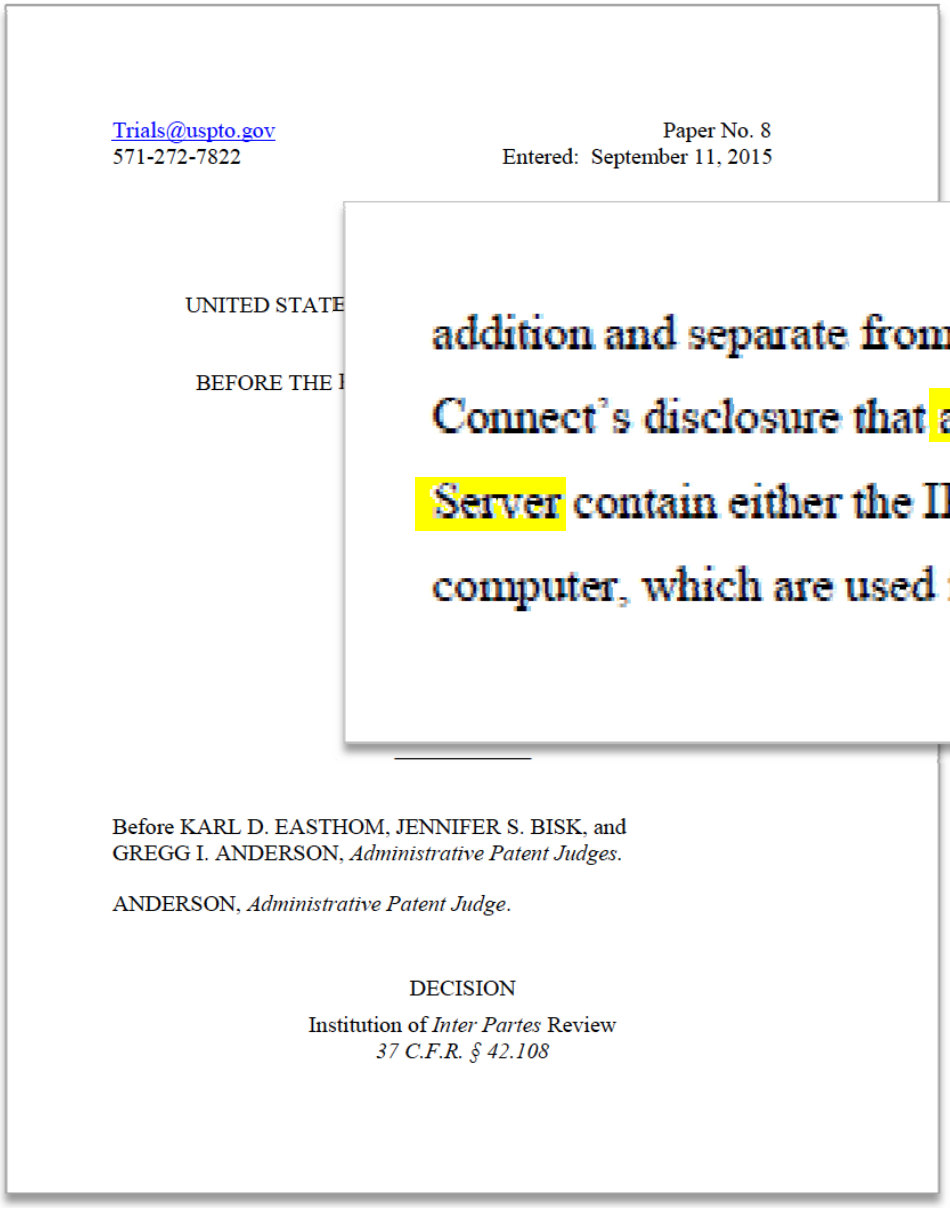
Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Petitioner also argues that Aventail Connect discloses step (1) of claim 1, "intercept[ing] . . . a request to look up an [] IP address corresponding to a domain name associated with the target . . . ." Pet. 31–33. Petitioner cites Aventail Connect's disclosure that a "client computer running Aventail Connect will transparently intercept each connection request made on the client." *Id.* at 31 (citing Ex. 1009, 7–9, 72–73; Ex. 1005 ¶¶ 171–172, 209–216). Petitioner cites to Aventail Connect's disclosure that to connect to a "Remote Host," i.e., the recited "*target device*," a Domain Name System (DNS) lookup converts the hostname into an Internet Protocol (IP) address. *Id.* (citing Ex. 1009, 8, 11, 91–92; Ex. 1005 ¶ 210). In

Decision (811) at 15

Institution Decision

"a request to look up an Internet Protocol (IP) address"



Trials@uspto.gov
571-272-7822

Paper No. 8
Entered: September 11, 2015

UNITED STATE

BEFORE THE I

Before KARL D. EASTHOM, JENNIFER S. BISK, and GREGG I. ANDERSON, *Administrative Patent Judges.*

ANDERSON, *Administrative Patent Judge.*

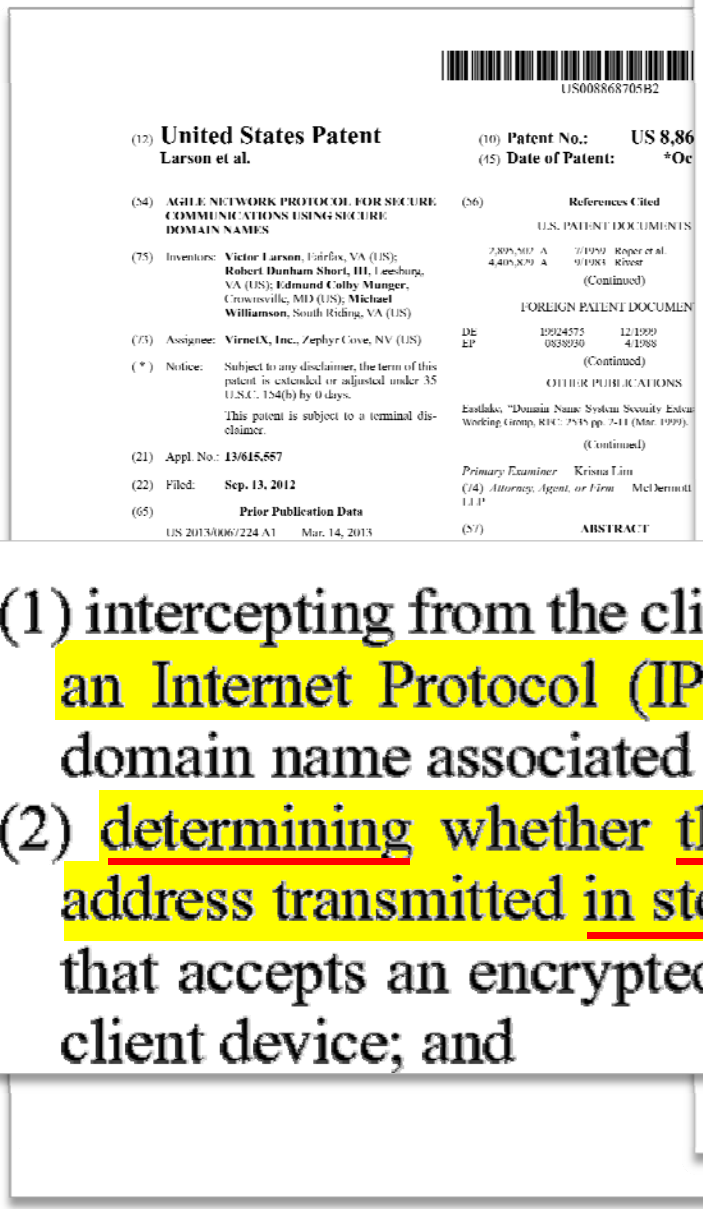
DECISION

Institution of *Inter Partes* Review
37 C.F.R. § 42.108

In addition and separate from the preceding, Petitioner cites to Aventail Connect's disclosure that all connection requests to the Aventail Extranet Server contain either the IP address or the domain name of the destination computer, which are used for handling and resolution. *Id.* at 32 (citing Ex.

Decision (811) at 15-16

’705 Patent, Claim 1



US008868705B2

(12) **United States Patent**
Larson et al.

(10) **Patent No.: US 8,86**
(45) **Date of Patent: *Oc**

(54) **AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmund Colby Munger**, Crownsville, MD (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **VirnetX, Inc.**, Zephyr Cove, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/615,557**

(22) Filed: **Sep. 13, 2012**

(65) **Prior Publication Data**

US 2013/0067224 A1 Mar. 14, 2013

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,305,537 A 7/1999 Roper et al.
4,405,829 A 9/1983 Rivest
(Continued)

FOREIGN PATENT DOCUMEN

DE 19924575 12/1999
EP 0838930 4/1988
(Continued)

OTHER PUBLICATIONS

Eastlake, "Domain Name System Security Exten
Working Group, RFC 2535 pp. 7-11 (Mar. 1999).
(Continued)

Primary Examiner Krisna Lim
(74) *Attorney, Agent, or Firm* McDermott
LLP

(57) **ABSTRACT**

1. A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the

at the request
responds to a
ications chan-
oviding provi-
he creation of
tween the cli-
the encrypted
data commu-
ices, the client
accesses the

encrypted communications channel.

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

’705 Patent (Ex. 1001) at Claim 1

Grounds Based on Aventail

"determining whether the request to look up the IP address [intercepted] in Step (1)…"

When the Aventail Connect LSP receives a connection request, it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) and/or encrypted (in SSL). When redirection and encryption are not necessary, Aventail Connect simply passes the connection request, and any subsequent transmitted data, to the TCP/IP stack.

Aventail (Ex. 1009) at 10
Pet. at 33-34

User authentication and encryption on the Aventail ExtraNet Server require all users to use Aventail Connect to authenticate and encrypt their sessions before any connection to the internal private network(s). For this example, the Aventail ExtraNet Server encrypts all sessions with SSL.

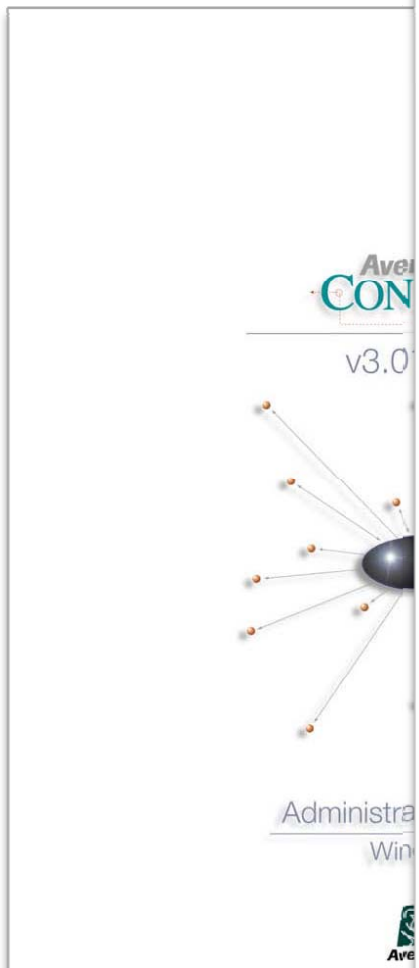
Aventail (Ex. 1009) at 73
Pet. at 34

Aventail

Petitioner Apple Inc. - Ex. 1009, Cover

Grounds Based on Aventail and RFC 2401

"determining whether the request to look up the IP address [intercepted] in Step (1)…"



How Does Aventail Connect Work?

The following three steps are identical to standard WinSock communications steps described above; however, nested inside them are additional actions and options introduced by Aventail Connect.

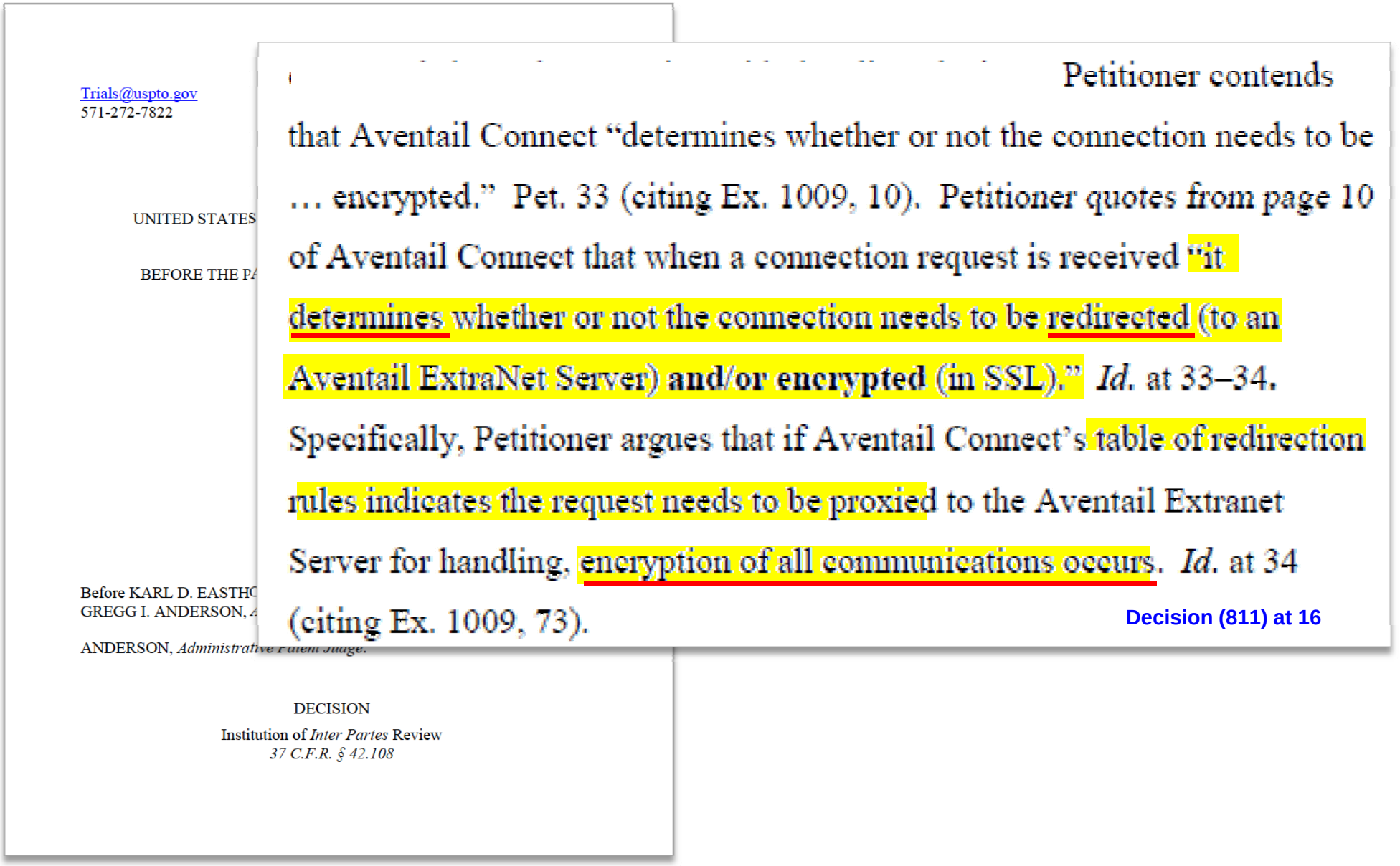
1. The application does a DNS lookup to convert the hostname to an IP address. If the application already knows the IP address, this entire step is skipped. Otherwise, Aventail Connect does the following:

   - If the hostname matches a local domain string or does not match a redirection rule, Aventail Connect passes the name resolution query through to the TCP/IP stack on the local workstation. The TCP/IP stack performs the lookup as if Aventail Connect were not running.
   - If the destination hostname matches a redirection rule domain name (i.e., the host is part of a domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution.
   - If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a fake DNS entry that it can recognize later, and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied, and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request.

Aventail (Ex. 1009) at 11-12

Institution Decision

"determining whether the request to look up the IP address [Intercepted] in Step (1)…"



Trials@uspto.gov
571-272-7822

UNITED STATES

BEFORE THE PA

Before KARL D. EASTHO
GREGG I. ANDERSON, A

ANDERSON, *Administrative Patent Judge.*

DECISION

Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Petitioner contends that Aventail Connect "determines whether or not the connection needs to be … encrypted." Pet. 33 (citing Ex. 1009, 10). Petitioner quotes from page 10 of Aventail Connect that when a connection request is received "it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) **and/or encrypted** (in SSL)." *Id.* at 33–34. Specifically, Petitioner argues that if Aventail Connect's table of redirection rules indicates the request needs to be proxied to the Aventail Extranet Server for handling, encryption of all communications occurs. *Id.* at 34 (citing Ex. 1009, 73).

Decision (811) at 16

Patent Owner Assertion

"determining whether the request to look up the IP address [intercepted] in Step (1)…"

Filed
By:
Jose
Pau
875
Wa
Tel
Fac
E-m

Petitioner's first proposition is incorrect because a domain name is never specified **in the connection request**. (Ex. 2016 at ¶¶ 29, 30.) Instead, the connection request includes an IP address, which is either the fake IP address that was previously returned by Aventail Connect (in step 1), a routable IP address, or a real IP address. (*See supra* section III.A.1; Ex. 1009 at 12; Ex. 2013 (steps 2, 2a(1), 2a(2), 2a(3), 2a(4)); Ex. 2016 at ¶ 30.)

Opposition at 18

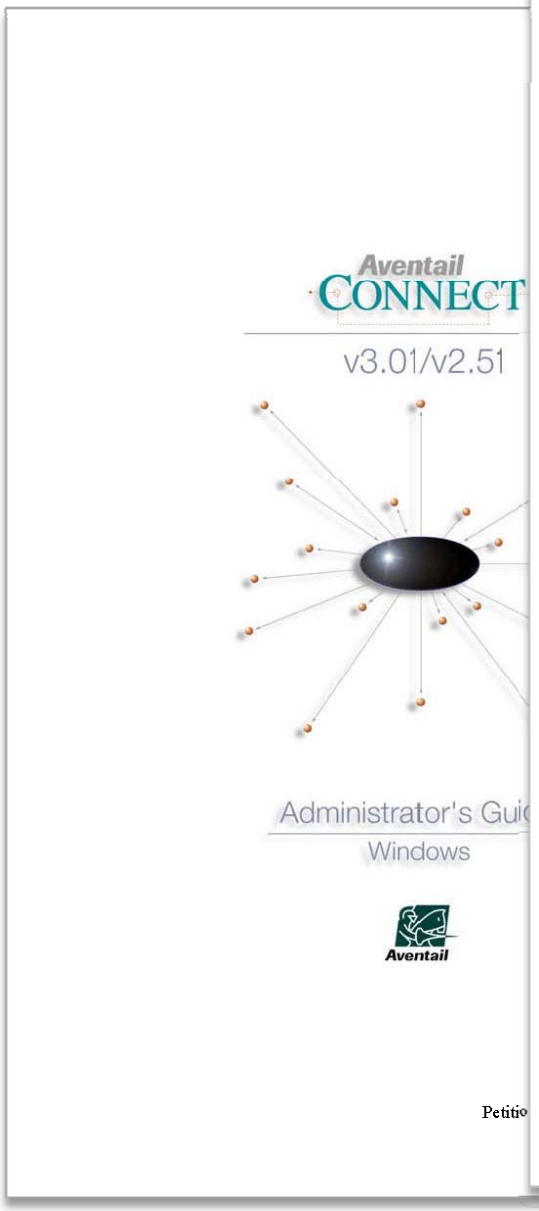
Patent Owner

Case IPR2015-00811
Patent 8,868,705

Patent Owner's Response

Grounds Based on Aventail

"determining whether the request to look up the IP address [intercepted] in Step (1)…"



2. The application requests a connection to the remote host. This causes the underlying stack to begin the TCP handshake. When the handshake is complete, the application is notified that the connection is established and that data may now be transmitted and received. Aventail Connect does the following:

   a. Aventail Connect checks the connection request.

      - If the request contains a false DNS entry (from step 1), it will be proxied.
      - If the request contains a routable IP address, and the rules in the configuration file say it must be proxied, Aventail Connect will call WinSock to begin the TCP handshake with the server designated in the configuration file.
      - If the request contains a real IP address and the configuration file rule says that it does not need to be proxied, the request will be passed to WinSock and processing jumps to step 3 as if Aventail Connect were not running.

   b. When the connection is completed, Aventail Connect begins the SOCKS negotiation.

      - It sends the list of authentication methods enabled in the configuration file.
      - Once the server selects an authentication method, Aventail Connect executes the specified authentication processing.
      - It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.

   c. When the SOCKS negotiation is completed, Aventail Connect notifies the application. From the application's point of view, the entire SOCKS negotiation, including the authentication negotiation, is merely the TCP handshaking.

Aventail (Ex. 1009) at 11-12

Patent Owner Assertion

"determining whether the request to look up the IP address [intercepted] in Step (1)…"

Filed on
By:
Joseph
Paul Ha
875 15t
Washin
Telepho
Facsimi
E-mail:

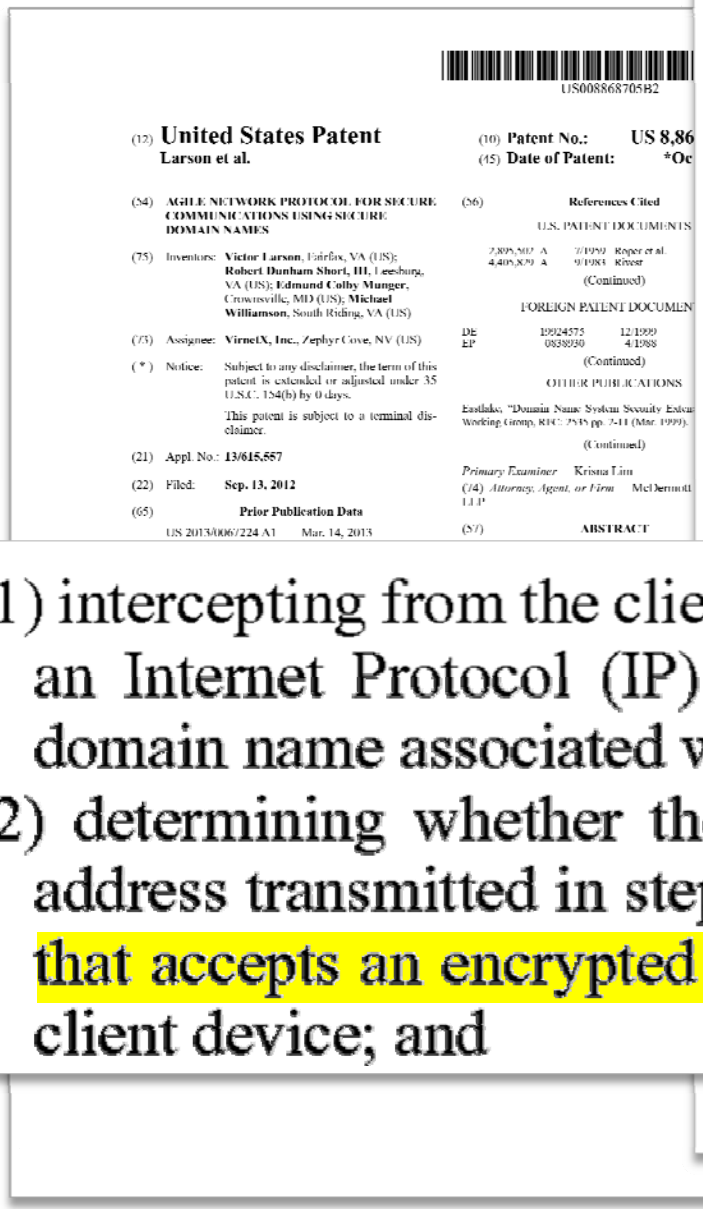
First, *Aventail* does not have any disclosure of a remote host accepting an encrypted connection. (Ex. 2016 at ¶ 34.) Indeed, as Petitioner acknowledges, *Aventail* does not disclose an encrypted connection *to the remote host* or target device. (Pet. at 39-43, "Aventail, thus, does not explicitly show that the entire path between the client device and the target device (**including the portion of path between the Extranet server and remote host**) remains encrypted" (emphasis added).)

Opposition at 20

Case IPR2015-00811
Patent 8,868,705

Patent Owner's Response

’705 Patent, Claim 1



US008868705B2

(12) **United States Patent**
Larson et al.

(10) **Patent No.: US 8,86**
(45) **Date of Patent: *Oc**

(54) **AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmund Colby Munger**, Crownsville, MD (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **VirnetX, Inc.**, Zephyr Cove, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/615,557**

(22) Filed: **Sep. 13, 2012**

(65) **Prior Publication Data**

US 2013/0067224 A1 Mar. 14, 2013

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,305,537 A 7/1999 Roper et al.
4,405,829 A 9/1983 Rivest
(Continued)

FOREIGN PATENT DOCUMEN

DE 19924575 12/1999
EP 0838930 4/1988
(Continued)

OTHER PUBLICATIONS

Eastlake, "Domain Name System Security Exten
Working Group, RFC 2535 pp. 7-11 (Mar. 1999).
(Continued)

Primary Examiner Krista Lin
(74) *Attorney, Agent, or Firm* McDermott
LLP

(57) **ABSTRACT**

1. A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the

hat the request
responds to a
ications chan-
oviding provi-
he creation of
tween the cli-
the encrypted
data commu-
ices, the client
accesses the

encrypted communications channel.

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

’705 Patent (Ex. 1001) at Claim 1

Institution Decision

"determining whether the request to look up the IP address [Intercepted] in Step (1)…"

Trials@uspt
571-272-782

UNI

BE

Before KAR
GREGG I. A

ANDERSON

The "determining" step states "determining whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device." All that is required is that the target device accepts an encrypted communication. Aventail Connect discloses that the connection request can be proxied and encrypted. *See* Pet. 33 (citing Ex. 1009, 73). Further, the Tamassia Declaration states, after analyzing Aventail Connect in detail, that "Aventail Connect will evaluate the redirection rule to determine *if the target host is one for which proxy redirection (and an encrypted communication)* through the Aventail Extranet Server is required." Ex. 1005 ¶ 237 (citing Ex. 1009, 11)(emphasis added). At this stage of the proceeding, and applying a reasonable likelihood standard of proof, Petitioner has shown that Aventail Connect determines whether the remote or target device accepts encrypted communication.

Decision (811) at 19

Grounds Based on Aventail and RFC 2401

"determining whether the request to look up the IP address [intercepted] in Step (1)…"

Even if the Board finds this "end-to-end" encryption to be a requirement of the claimed systems and methods, it would not render the claims patentable, as a person of ordinary skill would have considered deploying the Aventail system in a manner that provides end-to-end encryption to have been obvious based on the guidance in Aventail with RFC 2401. Section IV.B.2, below, provides the explanation of the basis of this conclusion of obviousness.

Pet. at 28

Patent Owner.

Patent No. 8,868,705

A person of ordinary skill in the art would have been motivated to implement the Aventail scheme to provide end-to-end encryption as described in RFC 2401, to thereby provide that the entire path from the client computer to the host on the remote network is encrypted. Ex. 1005 at ¶ 365-382.

Pet. at 41

Institution Decision

"determining whether the request to look up the IP address [Intercepted] in Step (1)…"

Petitioner acknowledges that "Aventail does not, however, expressly describe systems in which encrypted data sent by a client computer remains encrypted until it is received by the ultimate destination of that communication (so-called "end-to-end" encryption)." Pet. 39. Petitioner cites to RFC 2401 in its "Case 4" example, as teaching a configuration for sending encrypted network traffic through proxy or firewall computers, such as the Aventail Connect Extranet Server, without being decrypted, and then being decrypted remote computer. *Id.* at 40 (citing Ex. 1005 ¶ 364)(*see* Ex. 1008, 25–26 (Case 4)).

Decision (811) at 17

Trials@usp
571-272-78

UN

BE

Before KA
GREGG I.

ANDERSO

Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Institution Decision

"determining whether the request to look up the IP address [Intercepted] in Step (1)…"

Trials@uspto.gov
571-272-7822

Paper No. 8
Entered: September 11, 2015

Petitioner argues that one of ordinary skill in the art would combine RFC 2401 with Aventail Connect because Aventail Connect shows encryption over at least part of the connection path while RFC 2401 shows encryption over the entire connection path. Pet. 41 (citing Ex. 1005 ¶¶ 365–382). Patent Owner does not argue to the contrary.

Decision (811) at 18

Before
GREG

ANDERSON, *Administrative Patent Judge*.

DECISION

Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Patent Owner Assertion

"determining whether the request to look up the IP address [intercepted] in Step (1)…"

Paper No. _____
Filed: December 11, 2015

Filed on behalf of: VirnetX Inc.
By:

Second, determining whether a domain name in a DNS lookup request in step 1 matches a redirection rule for a destination (e.g., a remote host) is not the same as determining whether the remote host will accept an encrypted connection.

Opposition at 21

v.

VIRNETX INC.
Patent Owner

Case IPR2015-00811
Patent 8,868,705

Patent Owner's Response

Grounds Based on Aventail and RFC 2401

"determining whether the request to look up the IP address [intercepted] in Step (1)…"

When the Aventail Connect LSP receives a connection request, it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) and/or encrypted (in SSL). When redirection and encryption are not necessary, Aventail Connect simply passes the connection request, and any subsequent transmitted data, to the TCP/IP stack.

Aventail (Ex. 1009) at 10
Pet. at 33-34

User authentication and encryption on the Aventail ExtraNet Server require all users to use Aventail Connect to authenticate and encrypt their sessions before any connection to the internal private network(s). For this example, the Aventail ExtraNet Server encrypts all sessions with SSL.

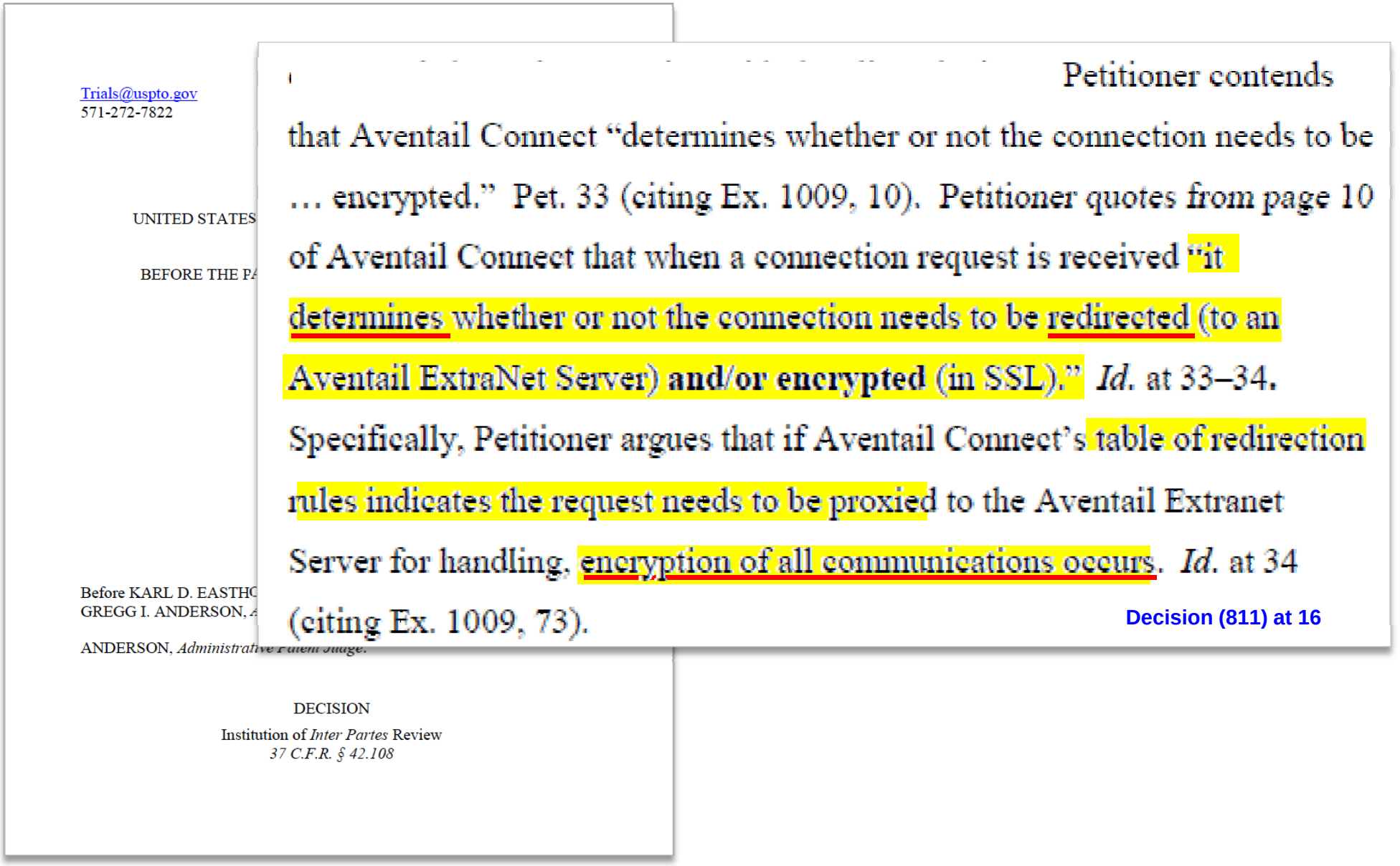
Aventail (Ex. 1009) at 73
Pet. at 34

Aventail

Petitioner Apple Inc. - Ex. 1009, Cover

Institution Decision

"determining whether the request to look up the IP address [Intercepted] in Step (1)…"



Trials@uspto.gov
571-272-7822

UNITED STATES

BEFORE THE PA

Before KARL D. EASTHO
GREGG I. ANDERSON, A

ANDERSON, *Administrative Patent Judge.*

DECISION

Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Petitioner contends that Aventail Connect "determines whether or not the connection needs to be … encrypted." Pet. 33 (citing Ex. 1009, 10). Petitioner quotes from page 10 of Aventail Connect that when a connection request is received "it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) **and/or encrypted** (in SSL)." *Id.* at 33–34. Specifically, Petitioner argues that if Aventail Connect's table of redirection rules indicates the request needs to be proxied to the Aventail Extranet Server for handling, encryption of all communications occurs. *Id.* at 34 (citing Ex. 1009, 73).

Decision (811) at 16

IPR2015-00811

1. Aventail and RFC 2401 Issues

A. Aventail and RFC 2401 teach "*Determining Whether the Request to Look Up the IP Address [Intercepted] in Step (1) . . . Corresponds to a Device that Accepts an Encrypted Channel Connection" (claims 1, 21)*

B. Aventail and RFC 2401 teach "*Encrypted Communications Channel Between the Client Device and the Target Device" (claims 1, 21)

C. Aventail and RFC 2401 teach *"In Response to Determining . . . Providing Provisioning Information"*

Patent Owner Assertion

"encrypted communications channel"

Paper No. _____

Filed: December 11, 2015

1001, claims 1 and 21.) In the context of the '705 patent claims, the encrypted communications channel between a client device and a target device is a *direct communications channel* that between the client device and the target device is encrypted. (*See supra* Section II.B.) *Aventail* does not, however, disclose such a direct channel between the client device and the remote host (the alleged "target device"). (Ex. 2016 at ¶¶ 38-40.)

Opposition at 23

Case IPR2015-00811
Patent 8,868,705

Patent Owner's Response

Grounds Based on Aventail and RFC 2401

"encrypted communications channel"

IPR2015-00811

Paper No. 29

The improper additional limitation Patent Owner seeks—that the encrypted communications channel be "direct"—has previously been rejected by the Board as unsupported by the prosecution history and Patent Owner's own statements, *see* IPR2014-00481, Paper 35 at 10, or because it was not necessary to resolve the case, *see* IPR2014-00482, Paper 34 at 4.

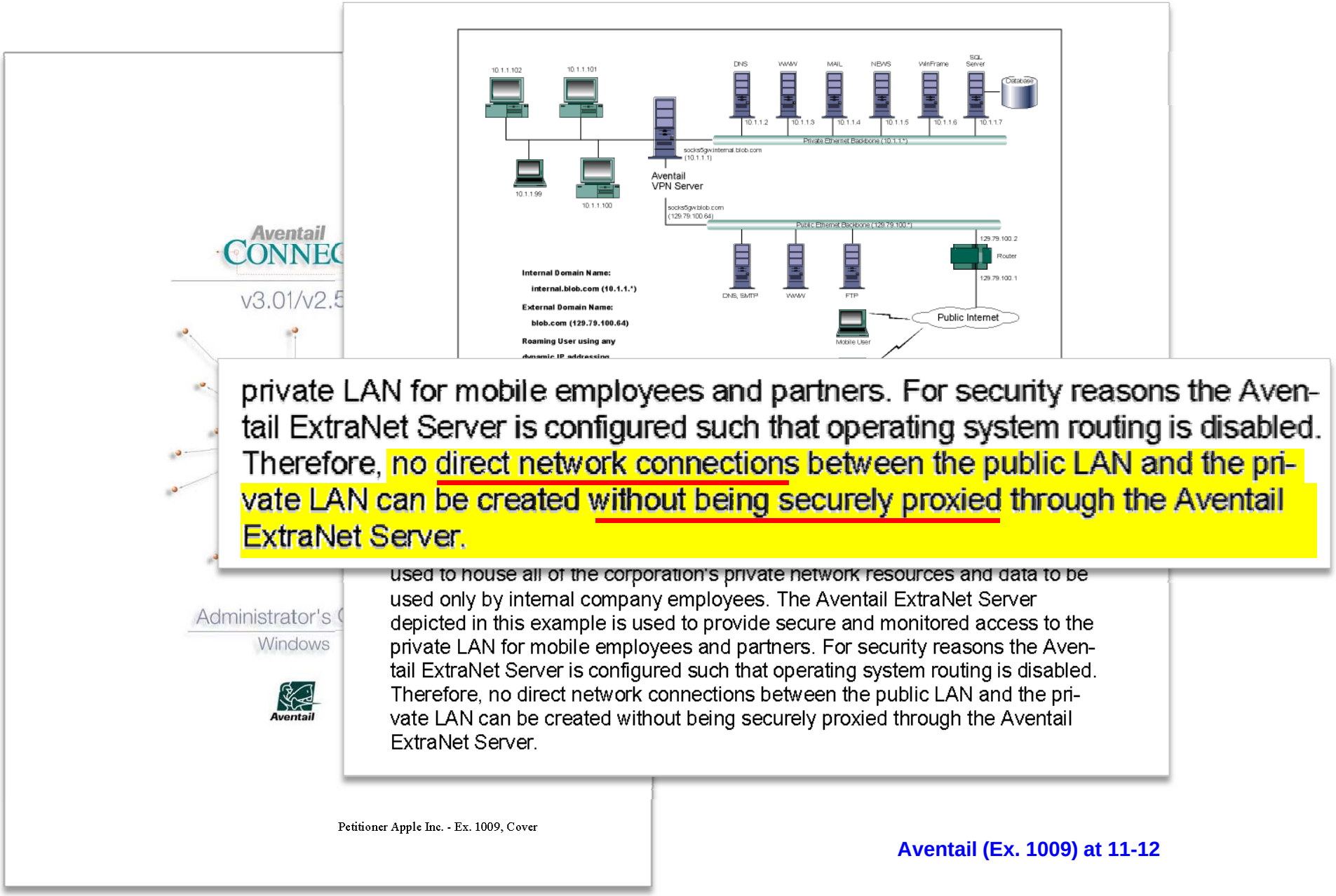
Reply at 3

Before KARL D. EASTHOM, JENNIFER S. BISK, and GREGG I. ANDERSON, *Administrative Patent Judges*.

PETITIONER'S REPLY

Grounds Based on Aventail and RFC 2401

"[Direct] encrypted communications channel"



private LAN for mobile employees and partners. For security reasons the Aventail ExtraNet Server is configured such that operating system routing is disabled. Therefore, no direct network connections between the public LAN and the private LAN can be created without being securely proxied through the Aventail ExtraNet Server.

used to house all of the corporation's private network resources and data to be used only by internal company employees. The Aventail ExtraNet Server depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners. For security reasons the Aventail ExtraNet Server is configured such that operating system routing is disabled. Therefore, no direct network connections between the public LAN and the private LAN can be created without being securely proxied through the Aventail ExtraNet Server.

Petitioner Apple Inc. - Ex. 1009, Cover

Aventail (Ex. 1009) at 11-12

Grounds Based on Aventail and RFC 2401

"[Direct] encrypted communications channel"

g) Secure Extranet Explorer

Aventail describes client computers running Aventail Connect that can dynamically browse and access resources within a private network once a secure connection had been established using a feature called "Secure Extranet Explorer (SEE)." Ex. 1009 at 90-101; Ex. 1005 ¶¶ 266-272. This functionality in Aventail Connect allows a remote user who had successfully established a VPN to a private network to see and access all of the network resources that user was authorized to access "just as [the user] would" using the Windows network neighborhood as a local user. Ex. 1009 at 91-92.

Pet. at 23-24
Aventail (Ex. 1009) at 90-101

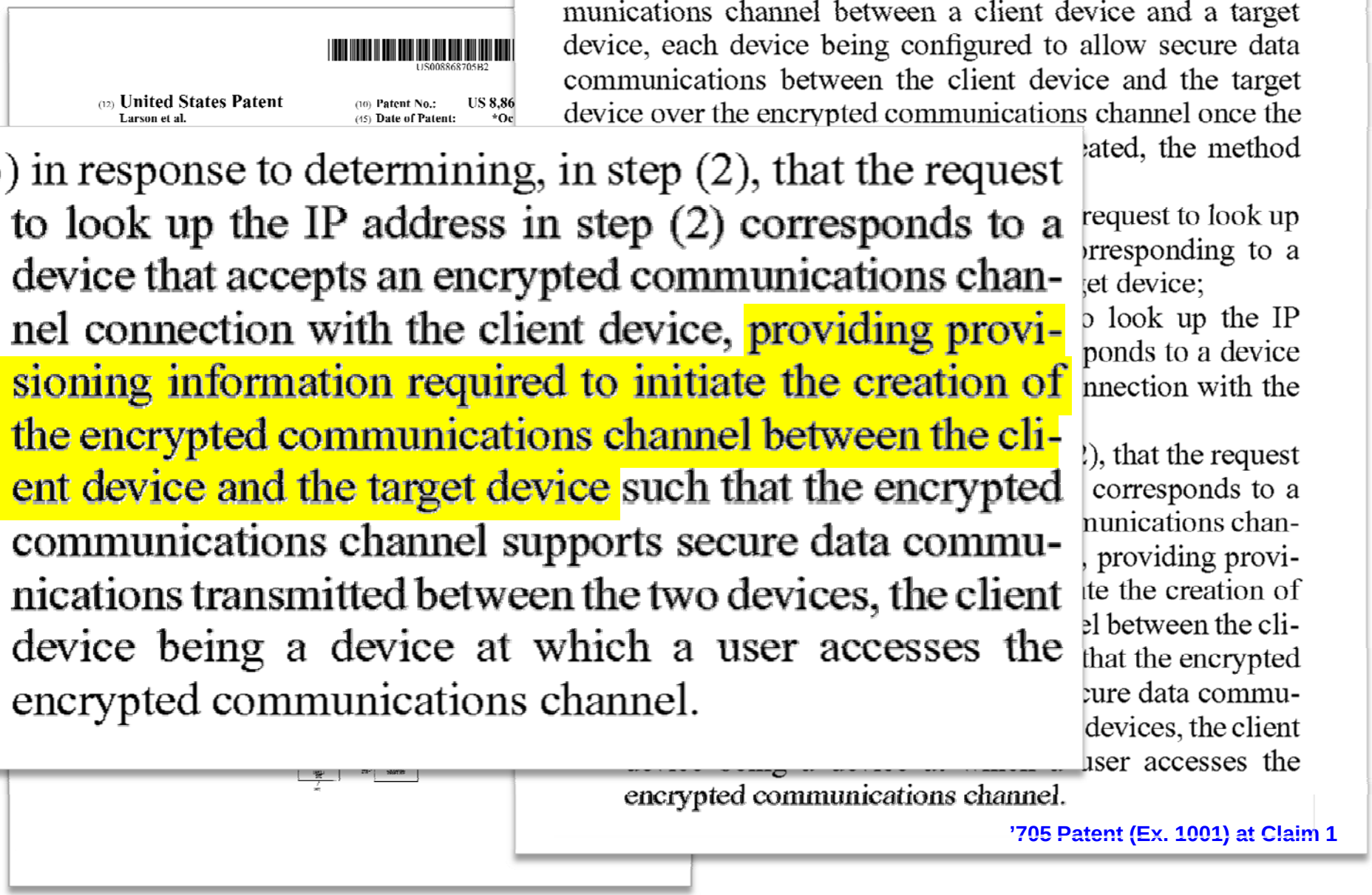
1. Aventail and RFC 2401 Issues

A. Aventail and RFC 2401 teach "*Determining Whether the Request to Look Up the IP Address [Intercepted] in Step (1) . . . Corresponds to a Device that Accepts an Encrypted Channel Connection" (claims 1, 21)*

B. Aventail and RFC 2401 teach "*Encrypted Communications Channel Between the Client Device and the Target Device" (claims 1, 21)*

C. Aventail and RFC 2401 teach *"In Response to Determining . . . Providing Provisioning Information" (claims 1, 21)*

’705 Patent, Claim 1



US008868705B2

(12) United States Patent
Larson et al.

(10) Patent No.: US 8,86
(15) Date of Patent: *Oc

1. A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the target device over the encrypted communications channel once the ...ated, the method

...request to look up
...rresponding to a
...et device;
...o look up the IP
...ponds to a device
...nnection with the

...), that the request
... corresponds to a
...unications chan-
..., providing provi-
...te the creation of
...el between the cli-
...that the encrypted
...cure data commu-
... devices, the client
...ser accesses the
encrypted communications channel.

(3) in response to determining, in step (2), that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel.

’705 Patent (Ex. 1001) at Claim 1

Institution

Construction of "provisioning information"

Trials@uspto.gov
571-272-7822

Paper No. 8
Entered: September 11, 2015

Accordingly, applying the broadest reasonable interpretation, we construe "provisioning information" to mean "information that is provided to enable or to aid in establishing a secure communications channel."

Decision (811) at 9

Case IPR2015-00811
Patent 8,868,705 B2

Before KARL D. EASTHOM, JENNIFER S. BISK, and GREGG I. ANDERSON, *Administrative Patent Judges.*

ANDERSON, *Administrative Patent Judge.*

DECISION

Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Institution Decision

"provisioning information"

Trials@uspto.gov
571-272-7822

UNITED S

BEFORE

Before KARL D. EASTHOM, JENNIFER S. BISK, and GREGG I. ANDERSON, *Administrative Patent Judges.*

ANDERSON, *Administrative Patent Judge.*

DECISION

Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Patent Owner concedes that Petitioner cites to instances where Aventail Connect discloses what Patent Owner contends are "provisioning information." Prelim. Resp. 20–21 (citing Pet. 35–38). However, Patent Owner contends the cited disclosures do not meet Petitioner's proposed construction of the term, "information that enables communication in **a virtual private network**, where the virtual private network uses encryption." *Id.* at 20 (citing Pet. 11–13).

Decision (811) at 19

Patent Owner Assertion

"provisioning information"

Patent Owner's Proposed Construction
Information that is used to establish an encrypted communications channel

Opposition at 10-11

Paper No. _____
Filed: December 11, 2015

en Modi
Hastings LLP
5th Street NW
ington, DC 20005

BEFORE THE PATENT TRIAL AND A

APPLE INC.
Petitioner

v.

Therefore, HOSTENT is not required to initiate the creation of the *encryption* connection because the encrypted connection can be established without HOSTENT being provided by Aventail Connect.

Opposition at 29

Petitioner's analysis is incorrect for the additional reason that it does not identify any relationship between an "*encrypted* connection" and HOSTENT (emphasis added). (Pet. at 36.)

Opposition at 29

Aventail and the RFC References are Prior Art

Declaration of Christopher A. Hopen

IN

In re Patent No

Munger et al.

Filed: Septem

For: ESTAB
COMM
ON A D
(DNS) I

3. Prior to HomePipe, I was affiliated with Aventail, Inc., until that company was acquired by SonicWall, Inc. in 2007. I helped co-found Aventail in 1996, and served as its Chief Technical Officer and Vice-President of Engineering from 1996 to 2007.

4. While I was affiliated with Aventail, I was involved in the design, development and distribution of all of Aventail's network security products.

DECLARATION OF CHRIS A. HOPEN UNDER 37 C.F.R. § 1.132

I, CHRIS HOPEN, do hereby declare and state:

1. I am a citizen of the United States, and reside in 19805 15th Avenue NW, Shoreline, Washington.

16. I estimate that Aventail distributed thousands of copies of the AEC v3.0 product (including the Administrator Guides for Aventail Connect and Extranet Center) during the first six months of 1999.

6. When paired with Aventail MobileVPN or PartnerVPN server products, Aventail AutoSOCKS would automatically establish a VPN to give the remote user access to secured network resources on a private network. The AutoSOCKS client and the server would automatically authenticate the remote user and encrypt all communications with the remote user.

Petition at 15-16
Reply at 21-22
Ex. 1023

Declaration of James Chester

In re Patent

Filed:

Issued:

Inventors:

For: EST
CO
ON
(DN

I, JAMES S

1. I am
A.

2. I am

3. In a
doc
-
-

A. My

4. I am
Proc
com

5. Fro
Mac
strategic initiatives overseeing design and implementation of secure networking services, architecture, and cost reductions for IBM worldwide and IBM clients. In that role, I evaluated network security products and services from many vendors, and for designing and implementing these products and services that IBM designed and implemented for its clients.

15. I recall that Aventail announced its AEC v3.0 product in the fall of 1998, and began distributing this product no later than mid-January of 1999. Because IBM was the largest user of Aventail VPN products, we would be one of the first companies to receive new versions of the Aventail products; both evaluation and production products. I was personally involved in Aventail's strategic planning and direction from March 1998.

16. The AEC v3.0 product included version 3.01/2.51 of the Aventail Connect software, and version 3.0 of the Aventail Extranet Server.

17. Exhibit C is a copy of the Administrator's Guide for Aventail Connect v3.01/2.51. I recall receiving Exhibit C with the AEC v3.0 product no later than July 1998.

18. At the time I received Exhibit C, I was under no obligation to keep this document secret or to not distribute it to others. Like earlier Aventail products, we distributed copies of the AutoSOCKS Administrator's Guide along the other printed materials that came with the Aventail AutoSOCKS/VPN Server to IBM clients to whom we deployed VPN solutions, and to IBM employees using the Aventail Connect v3.01/v2.51 client.

Petition at 15-17
Reply at 21-23
Ex. 1022

Declaration of Michael Allyn Fratto

12. Exhibit G is a copy of the Aventail Connect v3.01/2.51 Administrator's Guide ("Aventail Connect v3.01"). The Aventail Connect 3.01/2.51 Administrator's Guide was distributed with the AEC v3.0 product.

13. Aventail announced AEC v3.0 in August of 1998. See Exhibit H (PR Newswire, "Aventail Ships Directory-enabled Extranet Solution; Aventail Extranet Center V3.1 Available At www.aventail.com." (August 9, 1999)). The AEC v3.0 product was distributed by Aventail in the fall of 1998. See, for example, Exhibit I ("Intranet Applications: Briefs," Network World, at page 55 (October 19, 1998)).

14. I recall receiving Exhibit G with the Aventail Extranet Center v3.0 product in approximately October of 1998. The copy of Exhibit G that I received in October of 1998 was not marked as being confidential, and no restrictions were imposed on my use of it or information in it.

which are published on the Network Computing website.

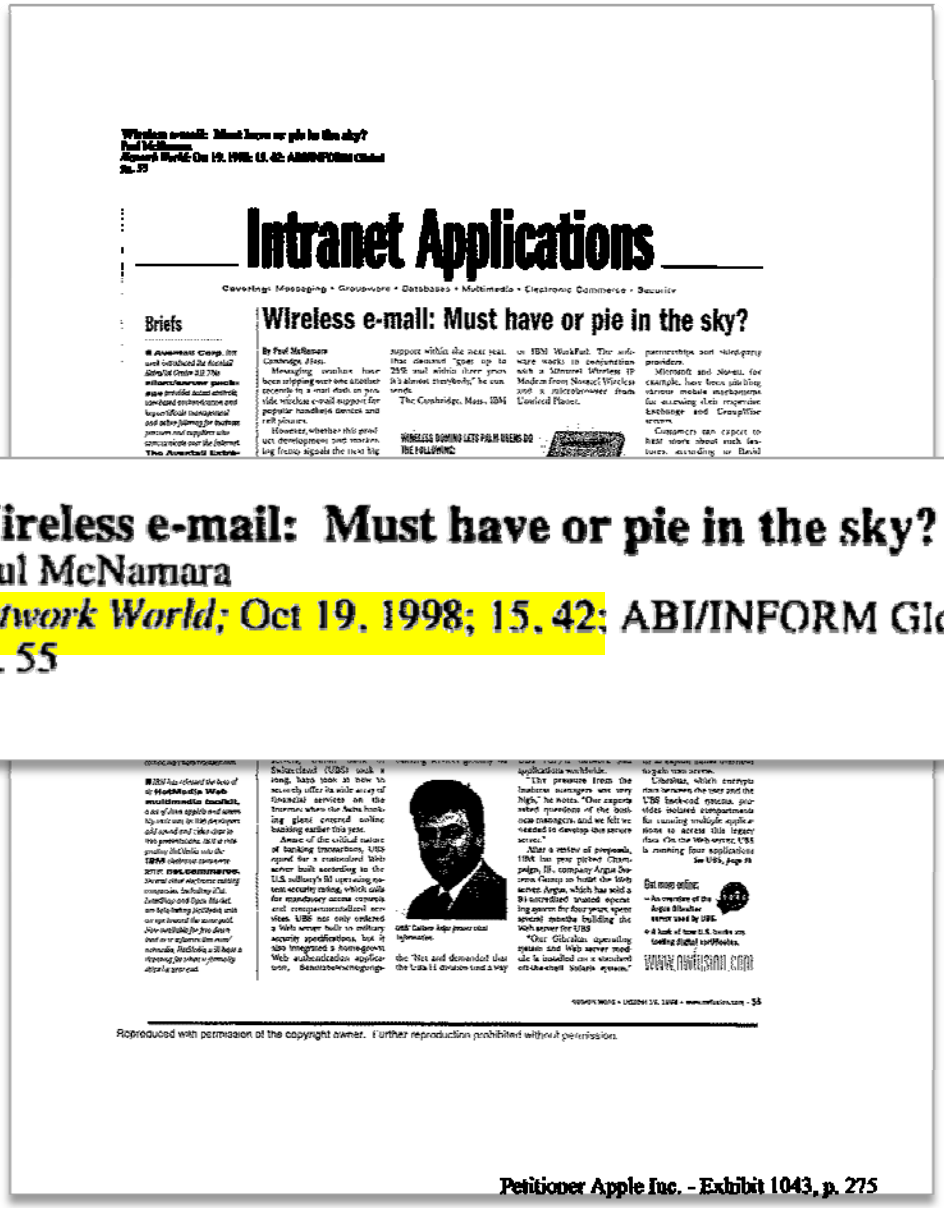
3. I presently serve as an adjunct faculty member of School of Information Studies at Syracuse University.

4. Since before 1999, I have had an extensive background and experience in network security systems, software and related technologies. I have been on staff of Network Computing conducting and writing comparative product reviews of networking and security products for the magazine, interviewing IT administrators and executives about networking and security issues trying to understand their needs. During the course of a review, I have to understand a problem set, understand technologies and standards that address a problem set, and create a set of comparative measures to asses a products ability to execute. I would set up a test network, verify its operation, conduct the tests, and ensure the results were accurate. In the 1997 to 2000 time frame, I focused on remote access products including modems, ISDN, and virtual private networking products, technologies, and standards as well as network and host-based firewalls.

5 I am being compensated for my time at a rate of $250.00 per hour

Petition at 15-17
Reply at 21-23
Ex. 1043

Exhibit I to
Declaration of Michael Allyn Fratto



Intranet Applications

Coverage: Messaging • Groupware • Databases • Multimedia • Electronic Commerce • Security

Briefs

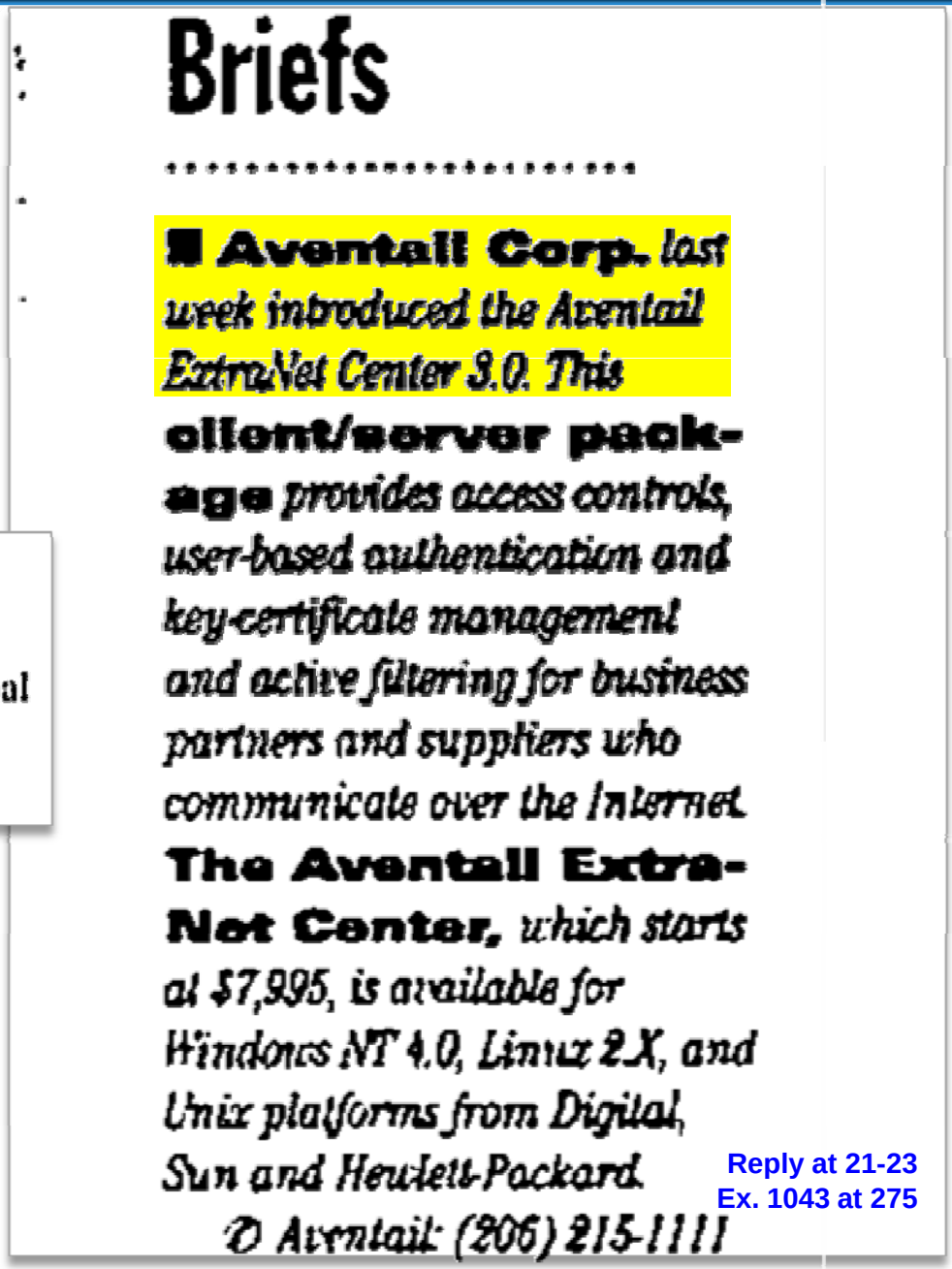
Wireless e-mail: Must have or pie in the sky?

By Paul McNamara

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Petitioner Apple Inc. - Exhibit 1043, p. 275

Wireless e-mail: Must have or pie in the sky?
Paul McNamara
Network World; Oct 19, 1998; 15, 42; ABI/INFORM Global
pg. 55



Briefs

■ **Aventail Corp.** *last week introduced the Aventail ExtraNet Center 3.0. This* **client/server package** *provides access controls, user-based authentication and key-certificate management and active filtering for business partners and suppliers who communicate over the Internet.* **The Aventail Extra-Net Center,** *which starts at $7,995, is available for Windows NT 4.0, Linux 2.X, and Unix platforms from Digital, Sun and Hewlett-Packard.* ✆ *Aventail: (206) 215-1111*

Reply at 21-23
Ex. 1043 at 275

RFCs

Petitioner's Expert, Dr. Tamassia

149. The way IETF RFC publications are prepared and released to the public in a formalized and structured process. In fact, the RFC development and publication process itself is described in an RFC – RFC 2026, dated October 1996. That RFC explains that that RFC publications and "Internet-Drafts" are widely disseminated on the Internet. For example, § 2.1 of RFC 2026 explains:

> Each distinct version of an Internet standards-related specification is published as part of the "Request for Comments" (RFC) document series. This archival series is the official publication channel for Internet standards documents and other publications of the IESG, IAB, and Internet community. RFCs can be obtained from a number of Internet hosts using anonymous FTP, gopher, World Wide Web, and other Internet document-retrieval systems.

Ex. 1036 (RFC 2026) at 6.

Ex. 1005 at ¶149; Ex. 1036 at 6; 811 Pet. at 24

Petitioner's Expert, Dr. Tamassia

Q. So are you familiar with the RFC process?

A. Yes.

Q. And what's the basis of your familiarity with the RFC process?

A. My business includes having viewed RFCs, having discussed RFCs, understanding for a while how the RFC process helps in general the developer community and manufacturers and researchers reach standards that facilitate the use of the Internet and, more generally, communications and computing.

Ex. 2015 at 103:1-13; Reply at 21

RFCs

NetworkWorld, Mar. 15, 1999

See the IETF documents RFC 2401 "Security Architecture for the Internet Protocol" at www.ietf.org/rfc/rfc2401.txt and RFC 2411 "IP Security Document Roadmap" at www.ietf.org/rfc/rfc2411.txt.

Ex. 1065 at 3; 810 Reply at 21

InfoWorld, Aug. 16, 1999

If it sounds like this is a lot of material to digest, it is: The Internet Engineering Task Force labored for several years on these IPsec documents. For starters, check out RFC 2411 (the document roadmap) and RFC 2401 (the security architecture), and then continue the research based on your network's specific security requirements.

All of these documents are available on the IETF Web site: www.ietf.org/rfc.html. ★

Ex. 1064 at 9; 810 Reply at 21

Beser and RFC 2401

to the '705 patent invalid. Paper 41 at 37-41 (May 11, 2015). The Board rejected Patent Owner's arguments that a person of ordinary skill would not have combined Beser and RFC 2401, (Paper 41 at 37-41), and that Beser does not disclose the step of "intercepting a request to lookup an IP address," (*id.* at 22-28). In the current

Reply at 2-3

U.S. Patent No. 8,868,705

Before KARL D. EASTHOM, JENNIFER S. BISK, and GREGG I. ANDERSON, *Administrative Patent Judges*.

PETITIONER'S REPLY BRIEF

Beser and RFC 2401

third-party network device 30. *Id.* In IPR2014-00237, the Board relied on this same request in finding that "Beser's trusted-third-party device 30 is 'informed of the request' from device 14; thereby 'receiving a request pertaining to a first entity [26] at another entity [14 or 30]' and satisfying the 'intercepting a request' element of claim 1 (and a similar element in claim 16)." Paper 41 at 24.

Reply at 8

Before KARL D. EASTHOM, JENNIFER S. BISK, and GREGG I. ANDERSON, *Administrative Patent Judges*.

PETITIONER'S REPLY BRIEF