Presentation of Petitioner Apple Inc.

IPR2015-00866
IPR2015-00868
IPR2015-00870
IPR2015-00871

U.S. Patent No. 8,458,341
U.S. Patent No. 8,516,131
U.S. Patent No. 8,560,705

Grounds

1. **IPR2015-00866 ('341 patent)**

   A. Ground 1: Whether Claims 1-11, 14-25, and 28 are obvious under 35 U.S.C. § 103 over Beser (Beser (Ex. 1007)) and RFC 2401 (Ex. 1008)

2. **IPR2015-00868 ('131 patent)**

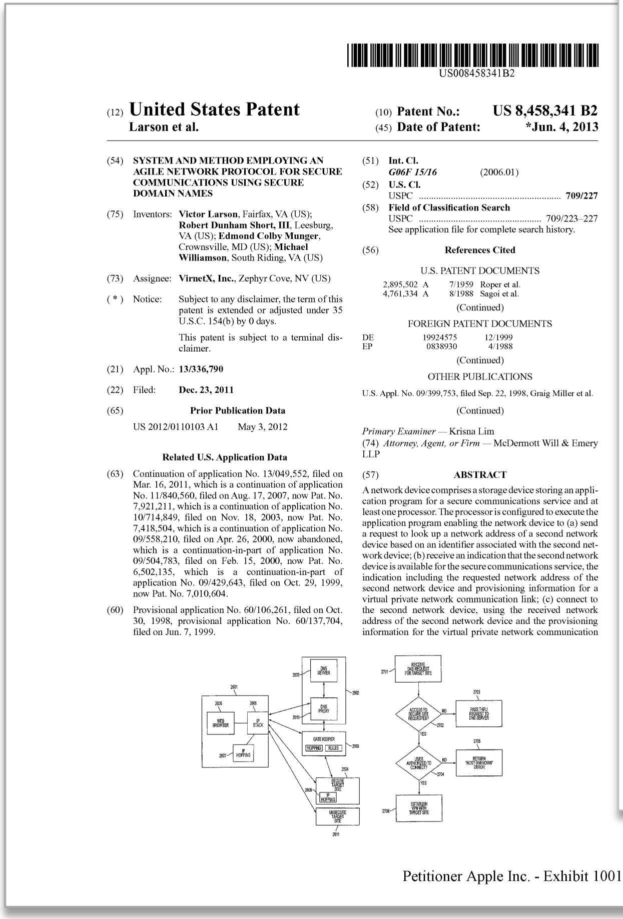
   A. Ground 1: Whether Claims 1-10,13-22, and 25-27 are obvious under 35 U.S.C. § 103 over Beser (Beser (Ex. 1007)) and RFC 2401 (Ex. 1008)

3. **IPR2015-00870 ('705 patent)**

   A. Ground 1: Whether Claims 1-23 and 25-30 are obvious under 35 U.S.C. § 103 over Beser (Beser (Ex. 1007)) and RFC 2401 (Ex. 1008)

   B. Ground 2: Whether Claim 24 is obvious under 35 U.S.C. § 103 over Beser, RFC 2401 and Brand (Ex. 1012)

’341 Patent, Claim 15



US008458341B2

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

(10) **Patent No.:** **US 8,458,341 B2**
(45) **Date of Patent:** ***Jun. 4, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,790**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0110103 A1 May 3, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,761,334	A	8/1988	Sagoi et al.

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

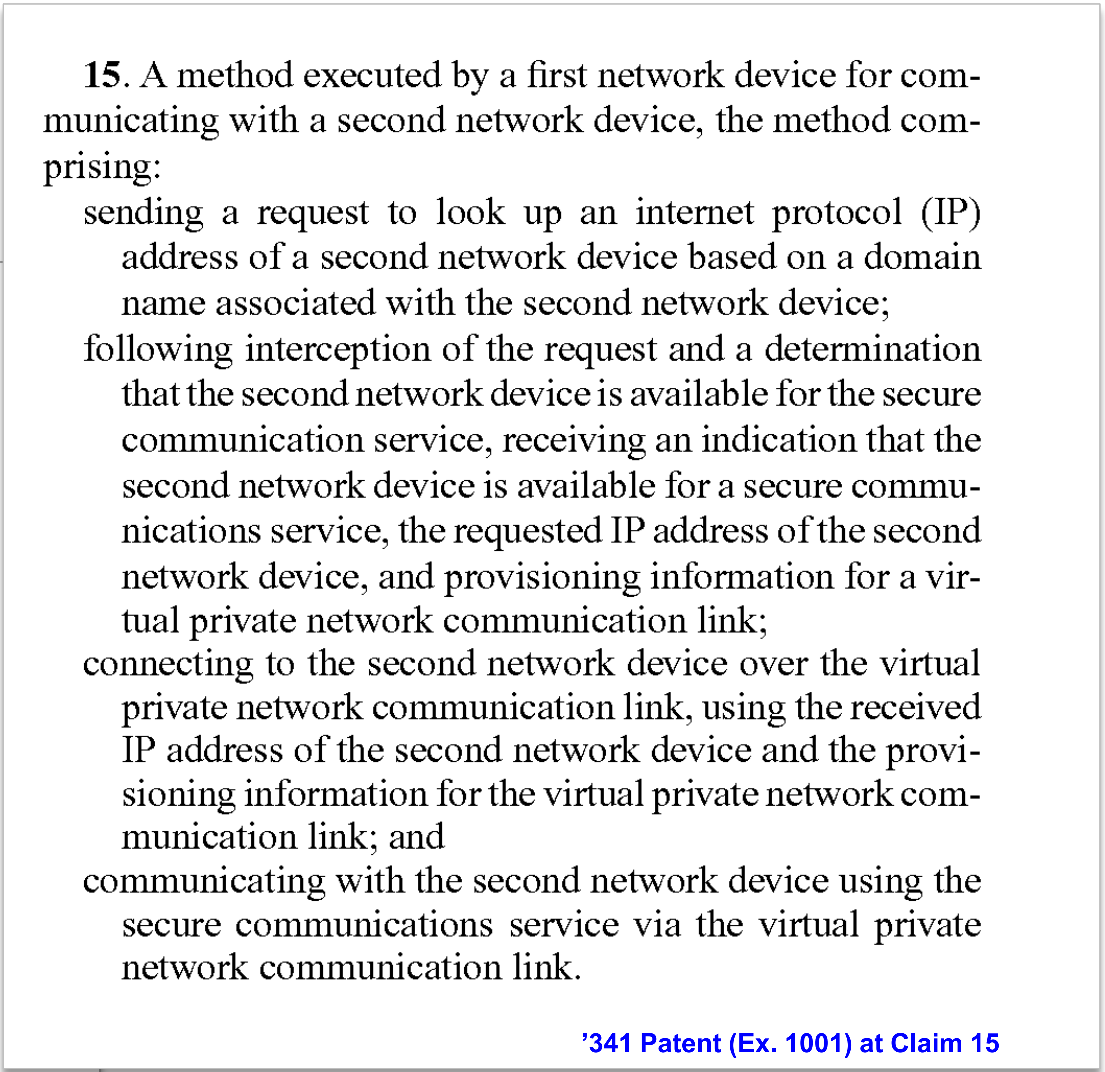
U.S. Appl. No. 09/399,753, filed Sep. 22, 1998, Graig Miller et al.

(Continued)

Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

A network device comprises a storage device storing an application program for a secure communications service and at least one processor. The processor is configured to execute the application program enabling the network device to (a) send a request to look up a network address of a second network device based on an identifier associated with the second network device; (b) receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link; (c) connect to the second network device, using the received network address of the second network device and the provisioning information for the virtual private network communication



15. A method executed by a first network device for communicating with a second network device, the method comprising:

sending a request to look up an internet protocol (IP) address of a second network device based on a domain name associated with the second network device;

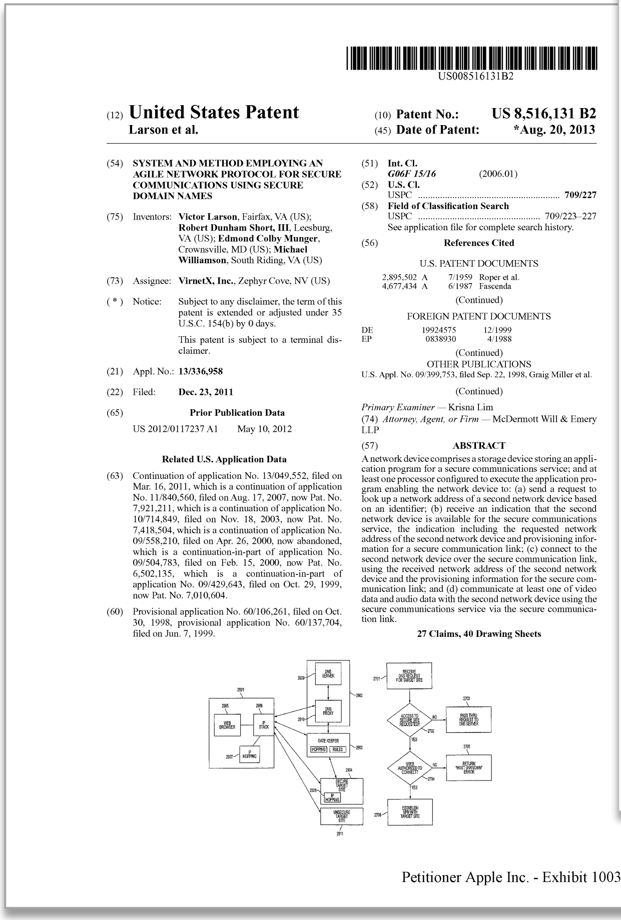
following interception of the request and a determination that the second network device is available for the secure communication service, receiving an indication that the second network device is available for a secure communications service, the requested IP address of the second network device, and provisioning information for a virtual private network communication link;

connecting to the second network device over the virtual private network communication link, using the received IP address of the second network device and the provisioning information for the virtual private network communication link; and

communicating with the second network device using the secure communications service via the virtual private network communication link.

’341 Patent (Ex. 1001) at Claim 15

’131 Patent, Claim 15



US008516131B2

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

(10) **Patent No.:** **US 8,516,131 B2**
(45) **Date of Patent:** ***Aug. 20, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,958**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0117237 A1 May 10, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,677,434	A	6/1987	Fascenda

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

U.S. Appl. No. 09/399,753, filed Sep. 22, 1998, Graig Miller et al.

(Continued)

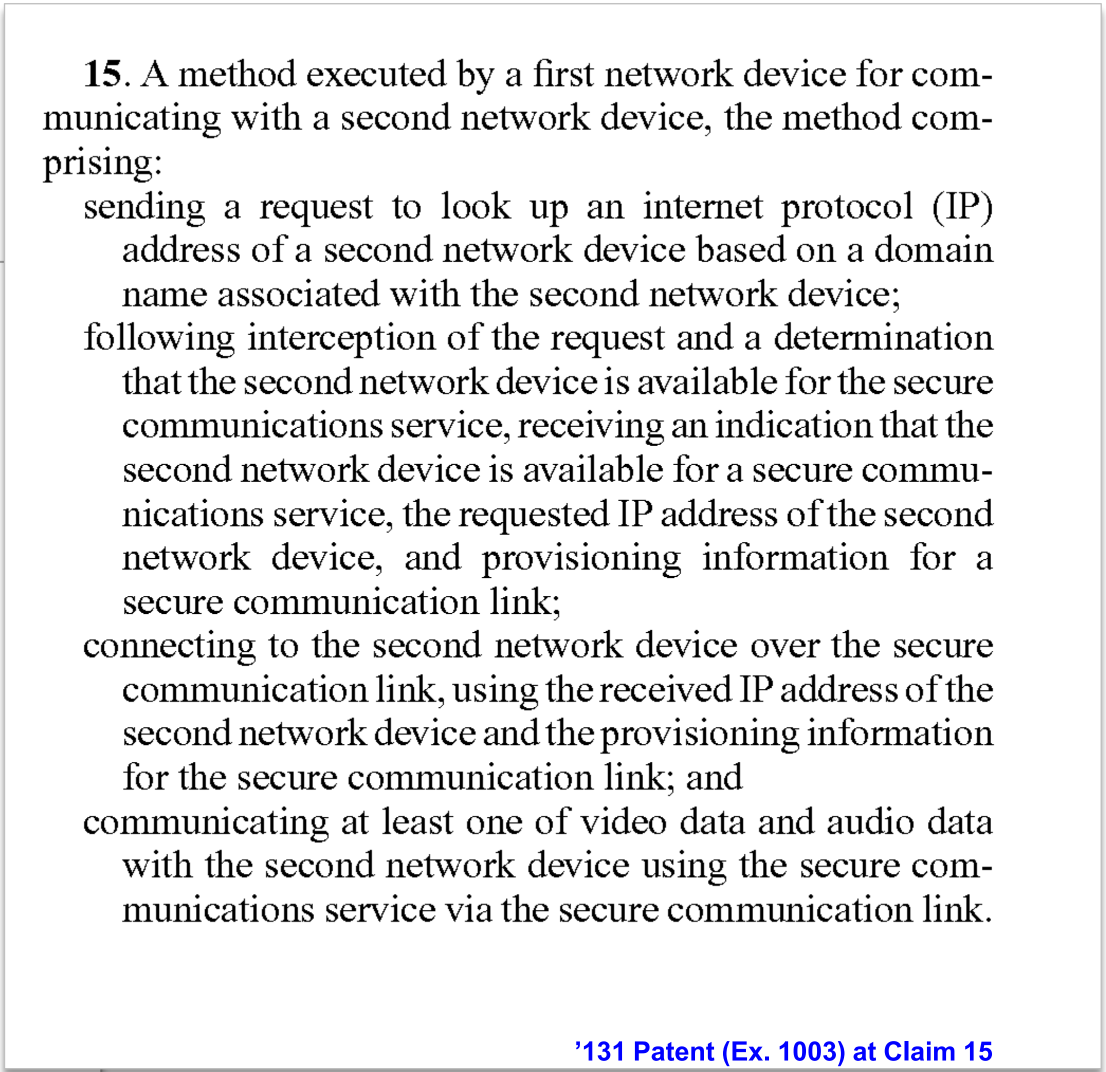
Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

A network device comprises a storage device storing an application program for a secure communications service; and at least one processor configured to execute the application program enabling the network device to: (a) send a request to look up a network address of a second network device based on an identifier; (b) receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a secure communication link; (c) connect to the second network device over the secure communication link, using the received network address of the second network device and the provisioning information for the secure communication link; and (d) communicate at least one of video data and audio data with the second network device using the secure communications service via the secure communication link.

27 Claims, 40 Drawing Sheets

Petitioner Apple Inc. - Exhibit 1003, p. 1



15. A method executed by a first network device for communicating with a second network device, the method comprising:

sending a request to look up an internet protocol (IP) address of a second network device based on a domain name associated with the second network device;

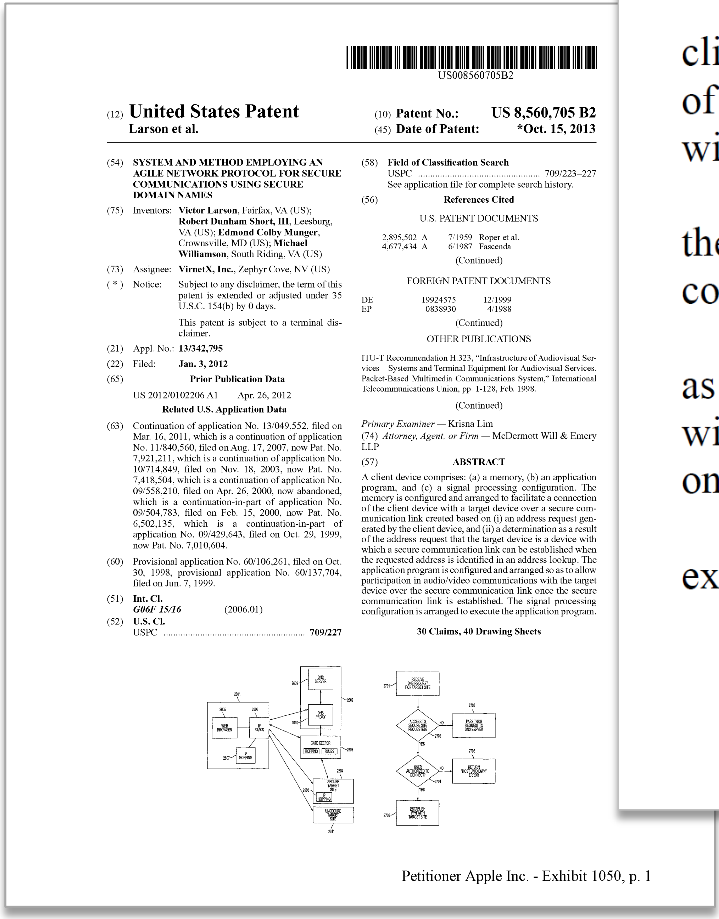
following interception of the request and a determination that the second network device is available for the secure communications service, receiving an indication that the second network device is available for a secure communications service, the requested IP address of the second network device, and provisioning information for a secure communication link;

connecting to the second network device over the secure communication link, using the received IP address of the second network device and the provisioning information for the secure communication link; and

communicating at least one of video data and audio data with the second network device using the secure communications service via the secure communication link.

’131 Patent (Ex. 1003) at Claim 15

’705 Patent, Claim 1



US008560705B2

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

(10) **Patent No.: US 8,560,705 B2**
(45) **Date of Patent: *Oct. 15, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/342,795**

(22) Filed: **Jan. 3, 2012**

(65) **Prior Publication Data**

US 2012/0102206 A1 Apr. 26, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,677,434	A	6/1987	Fascenda

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

ITU-T Recommendation H.323, “Infrastructure of Audiovisual Services—Systems and Terminal Equipment for Audiovisual Services. Packet-Based Multimedia Communications System,” International Telecommunications Union, pp. 1-128, Feb. 1998.

(Continued)

Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

A client device comprises: (a) a memory, (b) an application program, and (c) a signal processing configuration. The memory is configured and arranged to facilitate a connection of the client device with a target device over a secure communication link created based on (i) an address request generated by the client device, and (ii) a determination as a result of the address request that the target device is a device with which a secure communication link can be established when the requested address is identified in an address lookup. The application program is configured and arranged so as to allow participation in audio/video communications with the target device over the secure communication link once the secure communication link is established. The signal processing configuration is arranged to execute the application program.

30 Claims, 40 Drawing Sheets

Petitioner Apple Inc. - Exhibit 1050, p. 1

1. A client device comprising:

(a) memory configured and arranged to facilitate a connection of the client device with a target device over a secure communication link created based on

(i) interception of a request, generated by the client device, to look up an internet protocol (IP) address of the target device based on a domain name associated with the target device, and

(ii) a determination as a result of the request that the target device is a device with which a secure communication link can be established;

(b) an application program configured and arranged so as to allow participation in audio/video communications with the target device over the secure communication link once the secure communication link is established; and

(c) a signal processing configuration arranged to execute the application program.

Inst. Dec. at 5 (quoting ’705 Patent (Ex. 1050) at Claim 1)

IPR2015-00866, -868, -870

Beser and RFC 2401 Issues

1. **Common Issues (866, 868, & 870)**

   A. "Virtual Private Network Communication Link" (866: claims; 868: claim 10; 870: claims 6 & 21)

   B. Encrypting audio/visual data

   C. Combining Beser and RFC 2401 would have been obvious

   D. A "*request to look up an []IP address… based on a domain name associated with the second network [target] device*"

   E. "*Interception of the request to look up an Internet Protocol (IP) address*"

2. **Issues Affecting 866 & 868 Only**

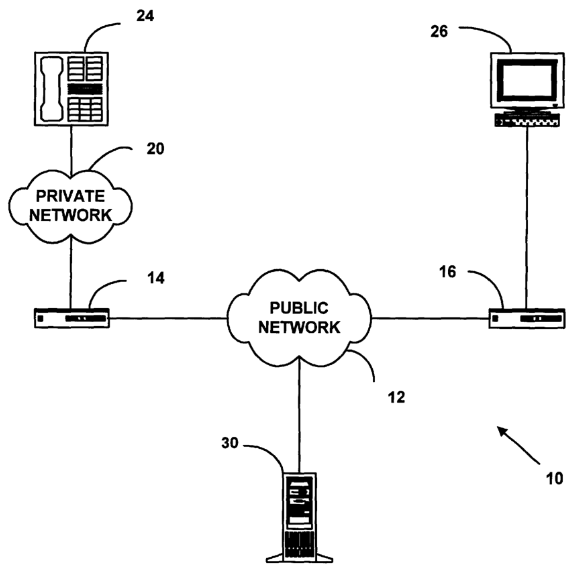
   A. "Receiv[ing]. . . An Indication [and] a Network Address"

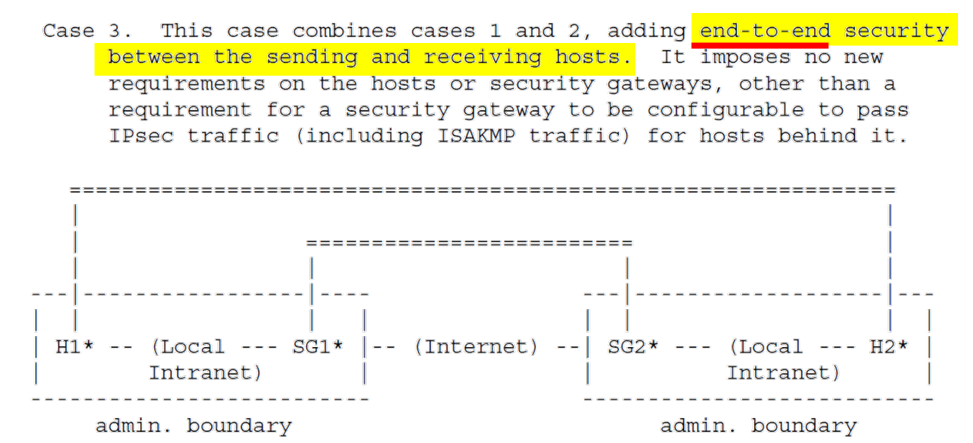
3. **Dependent Claims**

   A. "email" and "secure domain name"

Beser and RFC 2401 Grounds

FIG. 1



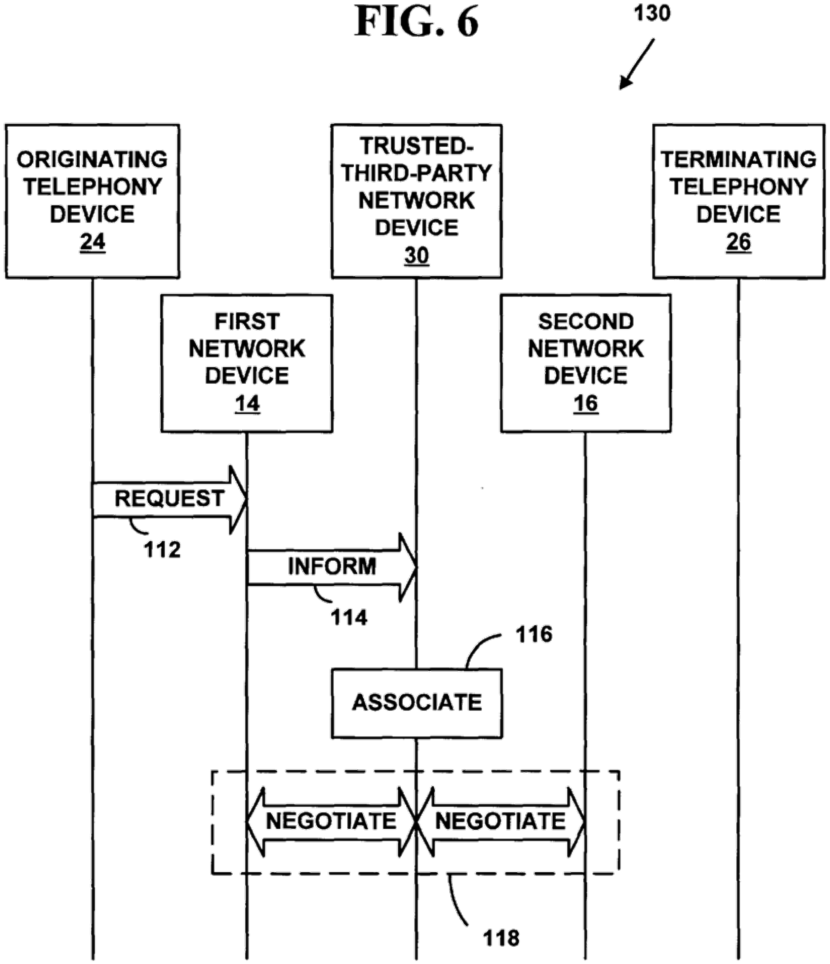


Case 3. This case combines cases 1 and 2, adding end-to-end security between the sending and receiving hosts. It imposes no new requirements on the hosts or security gateways, other than a requirement for a security gateway to be configurable to pass IPsec traffic (including ISAKMP traffic) for hosts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

```
   ================================================================
   |                                                              |
   |                 =========================                    |
   |                 |                       |                    |
---|-----------------|----                ---|--------------------|---
|  |                 |   |                |  |                    |  |
| H1* -- (Local --- SG1* |-- (Internet) --| SG2* --- (Local --- H2*  |
|        Intranet)       |                |          Intranet)       |
--------------------------                ----------------------------
     admin. boundary                            admin. boundary
```

RFC 2401 (Ex. 1008) at 25; Pet. (866) at 25-26

FIG. 6



Ex. 1007 (Beser) at Figs. 1 & 6; Pet. (866) at 18, 19

IPR2015-00866, -868, -870

Beser and RFC 2401 Issues

1. **Common Issues (866, 868, & 870)**

   A. ***"Virtual Private Network Communication Link" (866: claims; 868: claim 10; 870: claims 6 & 21)***

   B. Encrypting audio/visual data

   C. Combining Beser and RFC 2401 would have been obvious

   D. A "*request to look up an []IP address… based on a domain name associated with the second network [target] device*"

   E. "*Interception of the request to look up an Internet Protocol (IP) address*"

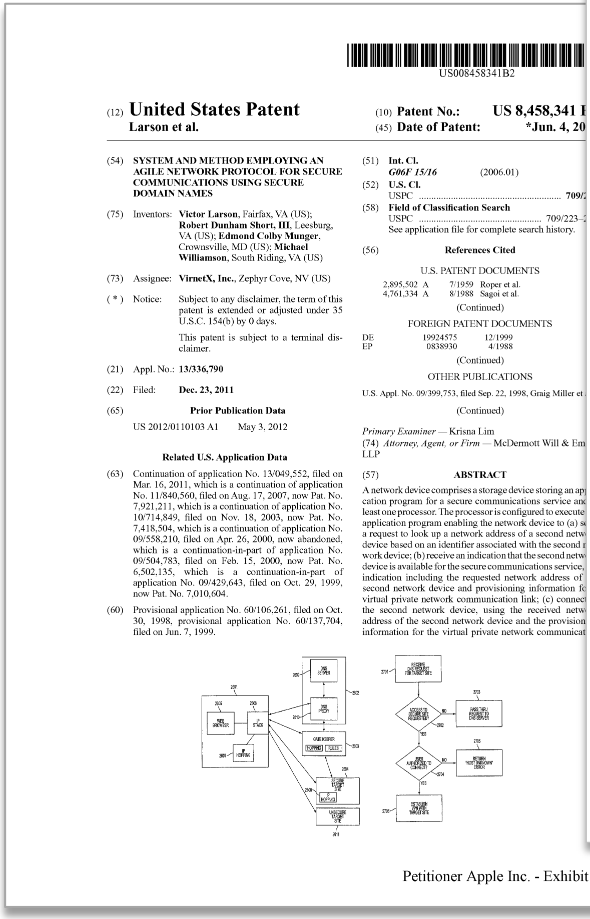
2. **Issues Affecting 866 & 868 Only**

   A. "Receiv[ing]. . . An Indication [and] a Network Address"

3. **Dependent Claims**

   A. "email" and "secure domain name"

The ’341 Claims:
a “*virtual private network communication link*”



US008458341B2

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

(10) **Patent No.:** **US 8,458,341 I**
(45) **Date of Patent:** ***Jun. 4, 20**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,790**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0110103 A1 May 3, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/**

(58) **Field of Classification Search**
USPC 709/223–
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,761,334	A	8/1988	Sagoi et al.

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

U.S. Appl. No. 09/399,753, filed Sep. 22, 1998, Graig Miller et

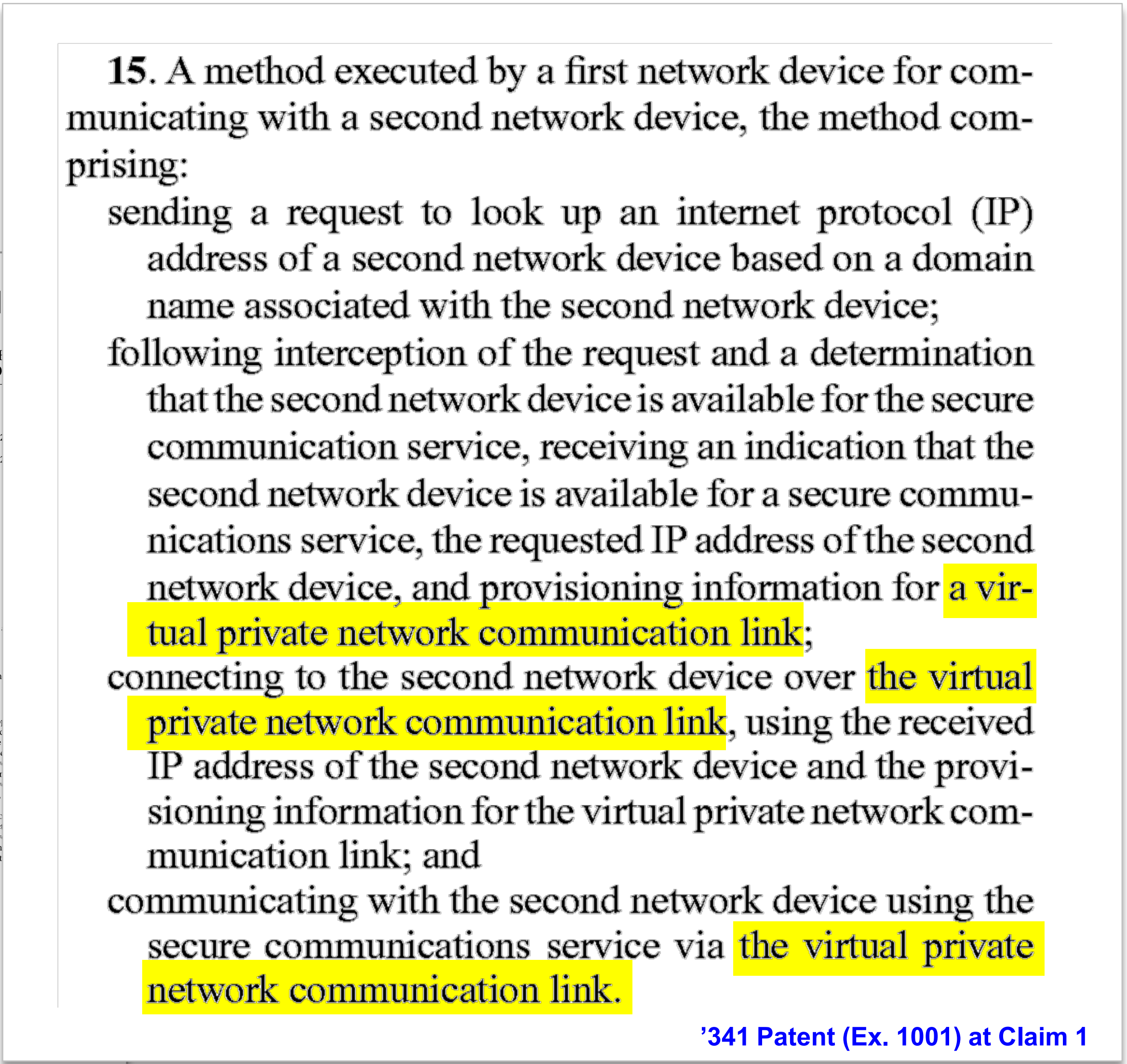
(Continued)

Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Em LLP

(57) **ABSTRACT**

A network device comprises a storage device storing an ap cation program for a secure communications service and least one processor. The processor is configured to execute application program enabling the network device to (a) se a request to look up a network address of a second netw device based on an identifier associated with the second n work device; (b) receive an indication that the second netw device is available for the secure communications service, indication including the requested network address of second network device and provisioning information fo virtual private network communication link; (c) connect the second network device, using the received netw address of the second network device and the provision information for the virtual private network communicat

Petitioner Apple Inc. - Exhibit 1001, p. 1



15. A method executed by a first network device for communicating with a second network device, the method comprising:

sending a request to look up an internet protocol (IP) address of a second network device based on a domain name associated with the second network device;

following interception of the request and a determination that the second network device is available for the secure communication service, receiving an indication that the second network device is available for a secure communications service, the requested IP address of the second network device, and provisioning information for a virtual private network communication link;

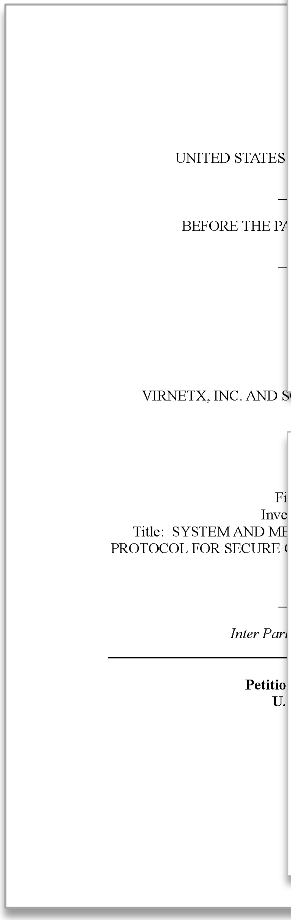
connecting to the second network device over the virtual private network communication link, using the received IP address of the second network device and the provisioning information for the virtual private network communication link; and

communicating with the second network device using the secure communications service via the virtual private network communication link.

’341 Patent (Ex. 1001) at Claim 1

Beser and RFC 2401

a "*virtual private network communication link*"


UNITED STATES

BEFORE THE PA

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

Fi
Inve
Title: SYSTEM AND ME
PROTOCOL FOR SECURE C

Inter Part

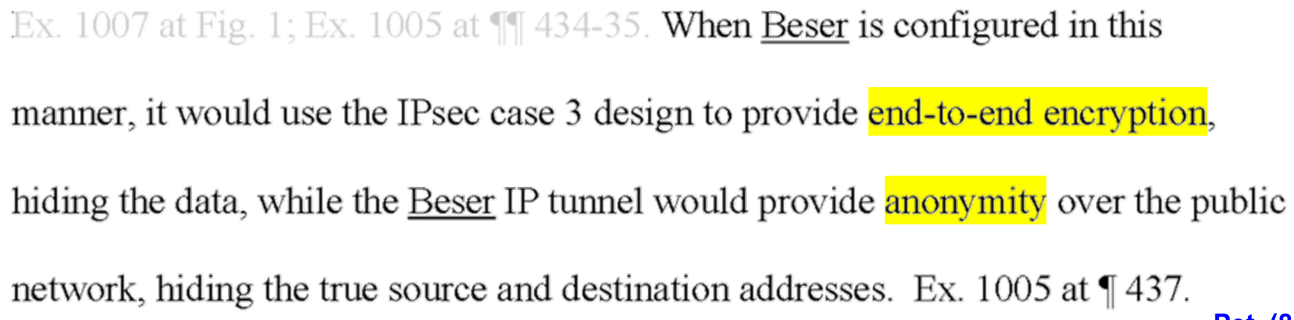
Petitio
U.

VPN Communication Link

Petitioner's Construction	**Patent Owner's Construction**
a transmission path between two devices that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping	a communication path between two devices in a virtual private network, where a virtual private network is a network of computers which privately and directly communicate with each other by encrypting traffic on insecure paths between the devices where the communication is both secure and anonymous

Pet. (866) at 14; Resp. (866) at 8

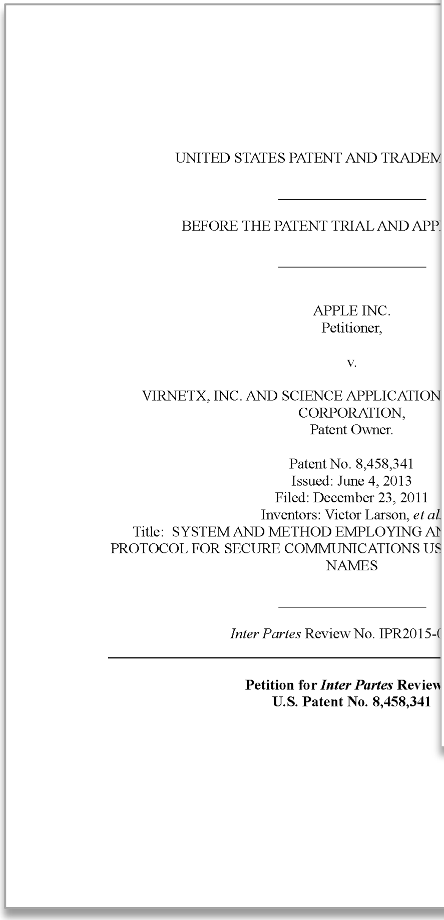
Petition


Ex. 1007 at Fig. 1; Ex. 1005 at ¶¶ 434-35. 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 ¶ 437.

Pet. (866) at 31

Beser and RFC 2401

a “*virtual private network communication link*”



UNITED STATES PATENT AND TRADEM

BEFORE THE PATENT TRIAL AND APP

APPLE INC.
Petitioner,

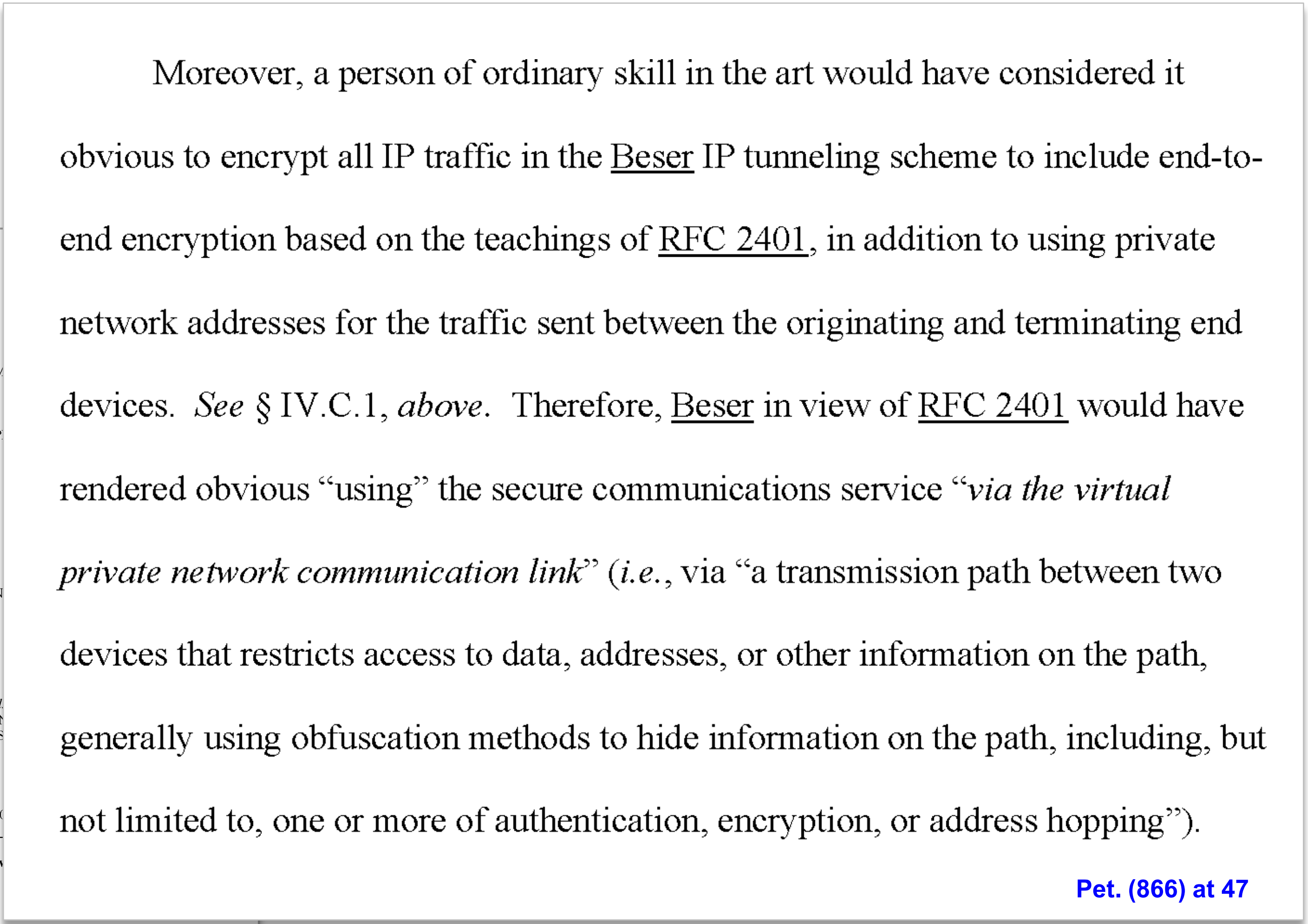
v.

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

Patent No. 8,458,341
Issued: June 4, 2013
Filed: December 23, 2011
Inventors: Victor Larson, *et al.*
Title: SYSTEM AND METHOD EMPLOYING AN
PROTOCOL FOR SECURE COMMUNICATIONS US
NAMES

Inter Partes Review No. IPR2015-(

Petition for *Inter Partes* Review
U.S. Patent No. 8,458,341

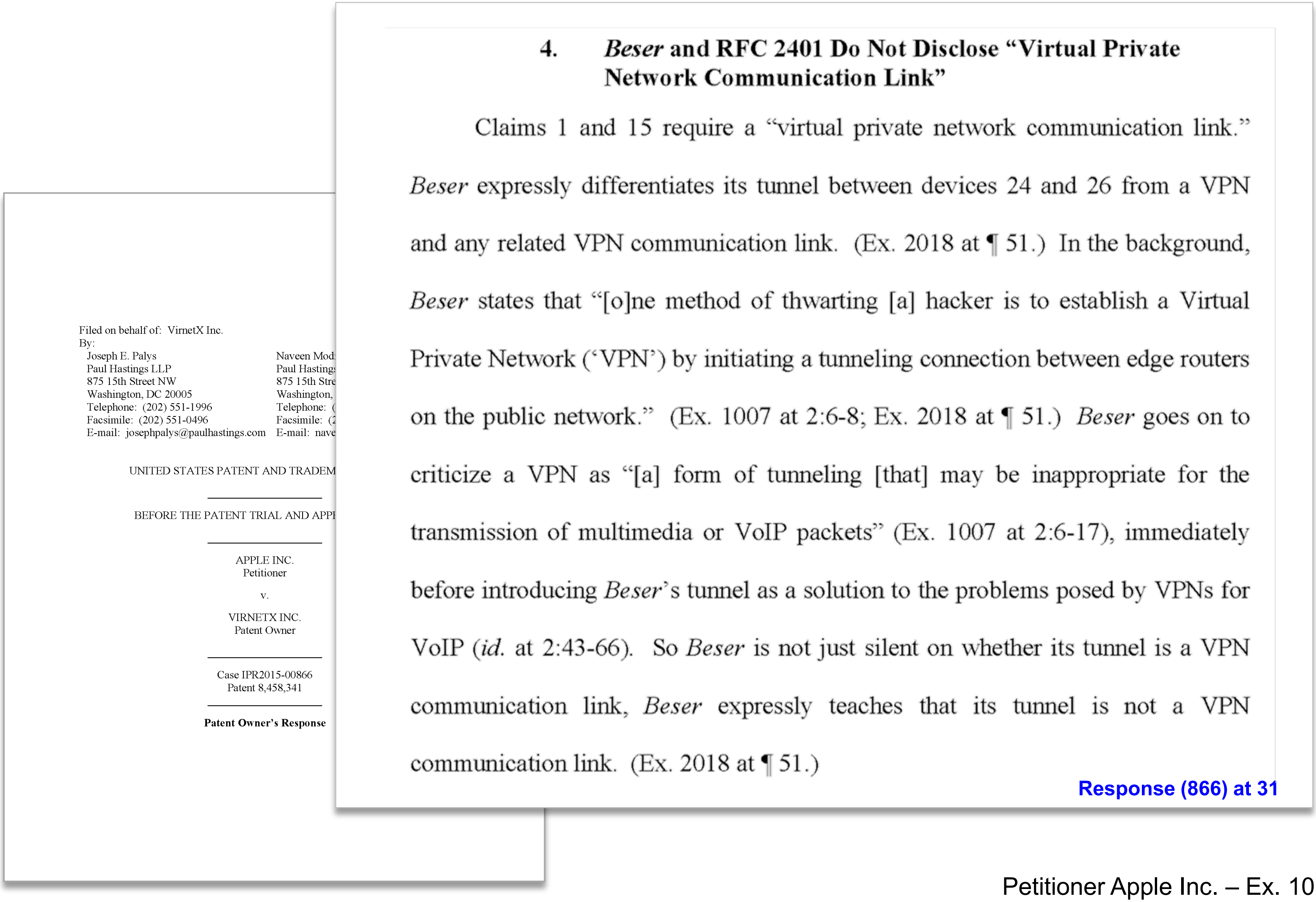


Moreover, a person of ordinary skill in the art would have considered it obvious to encrypt all IP traffic in the Beser IP tunneling scheme to include end-to-end encryption based on the teachings of RFC 2401, in addition to using private network addresses for the traffic sent between the originating and terminating end devices. *See* § IV.C.1, *above*. Therefore, Beser in view of RFC 2401 would have rendered obvious “using” the secure communications service “*via the virtual private network communication link*” (*i.e.*, via “a transmission path between two devices that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping”).

Pet. (866) at 47

Patent Owner Assertion

Patent Owner Does Not Address the Combination or its Claim Construction



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 Mod
Paul Hastings
875 15th Stre
Washington,
Telephone: (
Facsimile: (2
E-mail: nave

UNITED STATES PATENT AND TRADEM

BEFORE THE PATENT TRIAL AND APPE

APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2015-00866
Patent 8,458,341

Patent Owner's Response

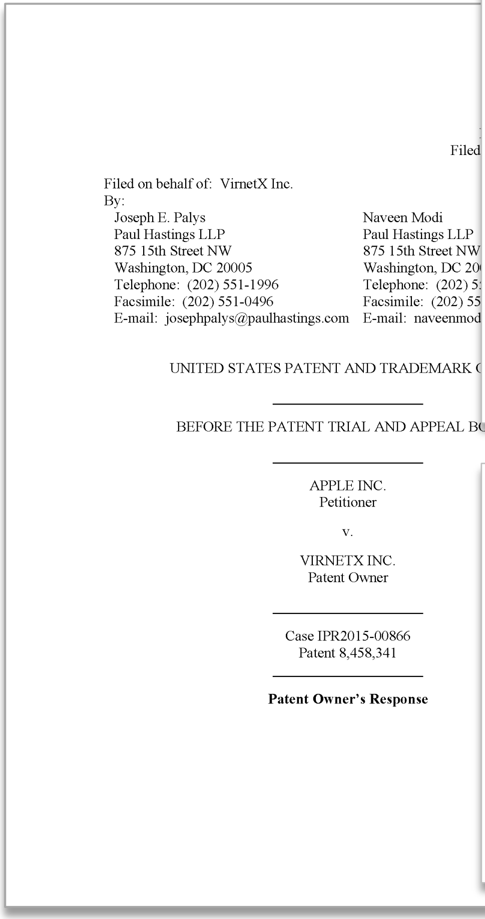
4. *Beser* and RFC 2401 Do Not Disclose "Virtual Private Network Communication Link"

Claims 1 and 15 require a "virtual private network communication link." *Beser* expressly differentiates its tunnel between devices 24 and 26 from a VPN and any related VPN communication link. (Ex. 2018 at ¶ 51.) In the background, *Beser* states that "[o]ne method of thwarting [a] hacker is to establish a Virtual Private Network ('VPN') by initiating a tunneling connection between edge routers on the public network." (Ex. 1007 at 2:6-8; Ex. 2018 at ¶ 51.) *Beser* goes on to criticize a VPN as "[a] form of tunneling [that] may be inappropriate for the transmission of multimedia or VoIP packets" (Ex. 1007 at 2:6-17), immediately before introducing *Beser*'s tunnel as a solution to the problems posed by VPNs for VoIP (*id.* at 2:43-66). So *Beser* is not just silent on whether its tunnel is a VPN communication link, *Beser* expressly teaches that its tunnel is not a VPN communication link. (Ex. 2018 at ¶ 51.)

Response (866) at 31

Patent Owner Admission

Virtual Private Network



Filed

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 Modi
Paul Hastings LLP
875 15th Street NW
Washington, DC 20
Telephone: (202) 5
Facsimile: (202) 55
E-mail: naveenmod

UNITED STATES PATENT AND TRADEMARK O

BEFORE THE PATENT TRIAL AND APPEAL BOARD

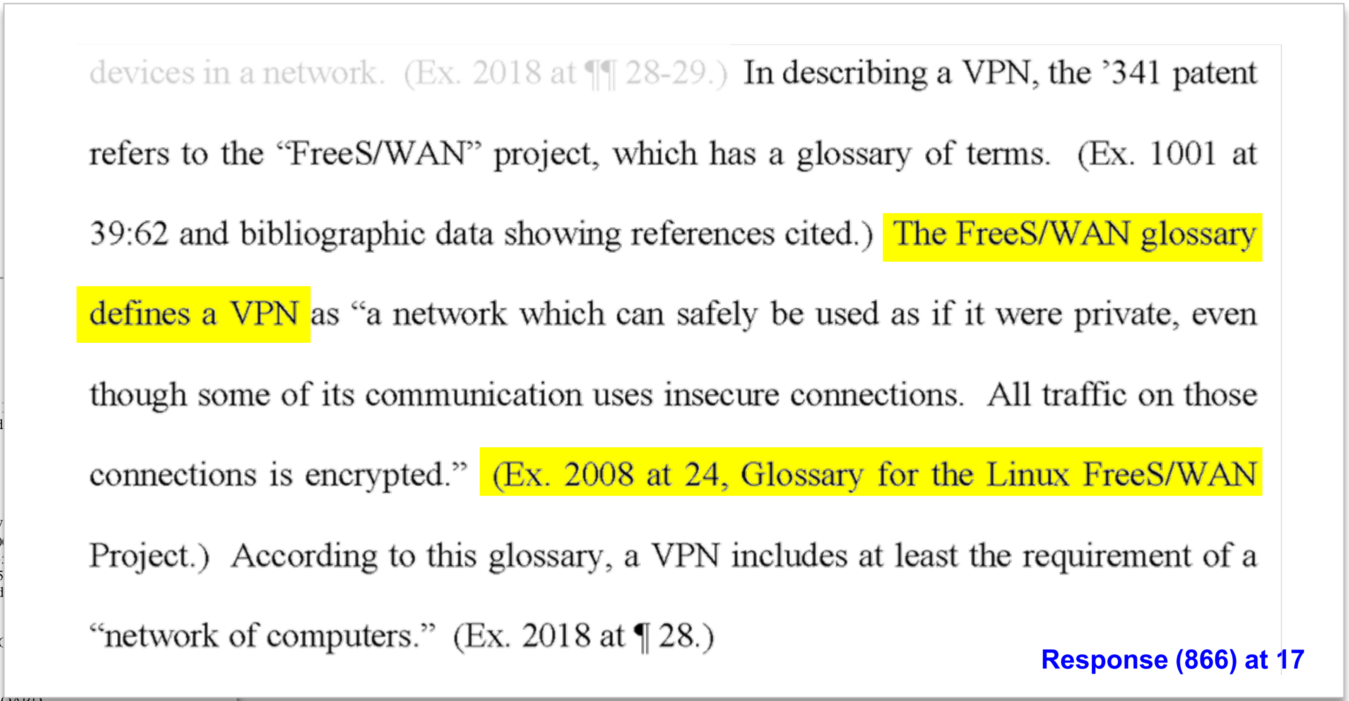
APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

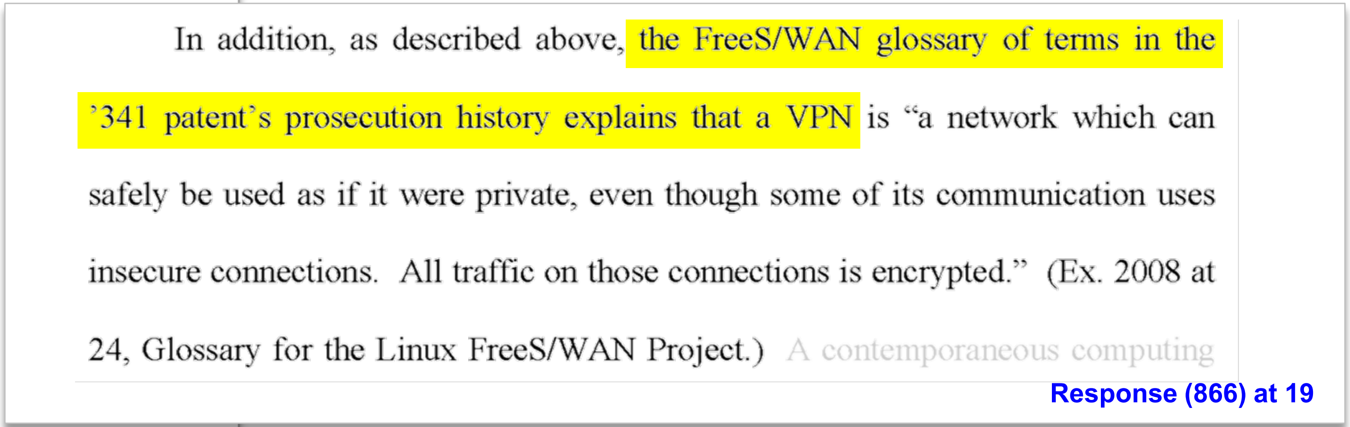
Case IPR2015-00866
Patent 8,458,341

Patent Owner's Response



devices in a network. (Ex. 2018 at ¶¶ 28-29.) In describing a VPN, the '341 patent refers to the "FreeS/WAN" project, which has a glossary of terms. (Ex. 1001 at 39:62 and bibliographic data showing references cited.) The FreeS/WAN glossary defines a VPN as "a network which can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted." (Ex. 2008 at 24, Glossary for the Linux FreeS/WAN Project.) According to this glossary, a VPN includes at least the requirement of a "network of computers." (Ex. 2018 at ¶ 28.)

Response (866) at 17



In addition, as described above, the FreeS/WAN glossary of terms in the '341 patent's prosecution history explains that a VPN is "a network which can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted." (Ex. 2008 at 24, Glossary for the Linux FreeS/WAN Project.) A contemporaneous computing

Response (866) at 19

Patent Owner Admission

Virtual Private Network

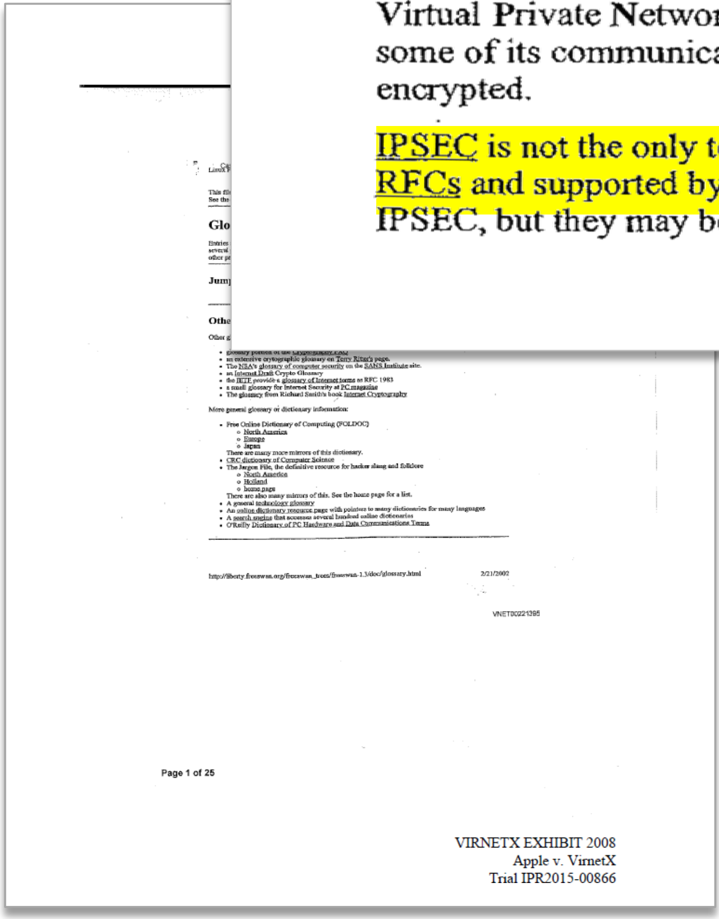
Glossary for the Linux FreeS/WAN project

VPN

Virtual Private Network, a network which can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted.

IPSEC is not the only technique available for building VPNs, but it is the only method defined by RFCs and supported by many vendors. VPNs are by no means the only thing you can do with IPSEC, but they may be the most important application for many users.

Ex. 2008 at 24-25; Reply (866) at 15



Linux F

This fil
See the

Glo

Entries
several
other p

Jum

Othe

Other g

- glossary portion of the Cryptography FAQ
- an extensive cryptographic glossary on Terry Ritter's page.
- The NSA's glossary of computer security on the SANS Institute site.
- an Internet Draft Crypto Glossary
- the IETF provide a glossary of Internet terms as RFC 1983
- a small glossary for Internet Security at PC magazine
- The glossary from Richard Smith's book Internet Cryptography

More general glossary or dictionary information:

- Free Online Dictionary of Computing (FOLDOC)
  - North America
  - Europe
  - Japan

  There are many more mirrors of this dictionary.
- CRC dictionary of Computer Science
- The Jargon File, the definitive resource for hacker slang and folklore
  - North America
  - Holland
  - home page

  There are also many mirrors of this. See the home page for a list.
- A general technology glossary
- An online dictionary resource page with pointers to many dictionaries for many languages
- A search engine that accesses several hundred online dictionaries
- O'Reilly Dictionary of PC Hardware and Data Communications Terms

http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/glossary.html 2/21/2002

VNET00221395

Page 1 of 25

VIRNETX EXHIBIT 2008
Apple v. VirnetX
Trial IPR2015-00866

IPR2015-00866, -868, -870

Beser and RFC 2401 Issues

1. **Common Issues (866, 868, & 870)**

   A. *“Virtual Private Network Communication Link”* (866: claims; 868: claim 10; 870: claims 6 & 21)

   B. Encrypting audio/visual data

   C. Combining Beser and RFC 2401 would have been obvious

   D. A “*request to look up an []IP address… based on a domain name associated with the second network [target] device”*

   E. “*Interception of the request to look up an Internet Protocol (IP) address”*

2. **Issues Affecting 866 & 868 Only**

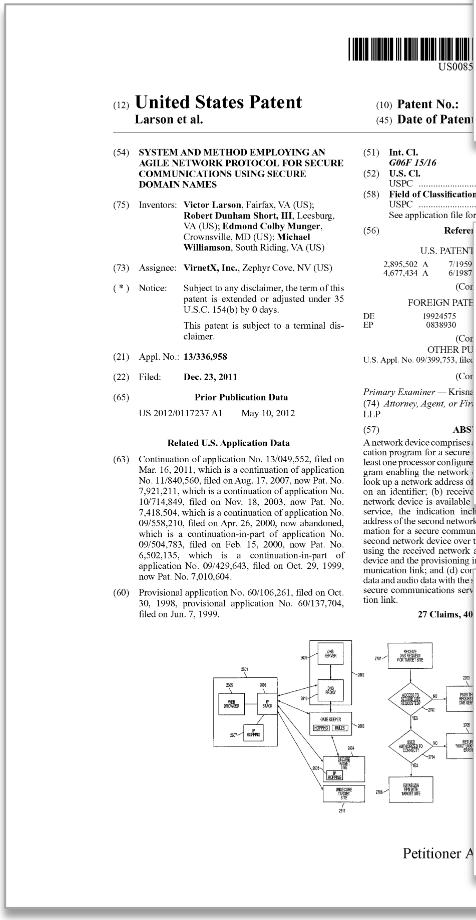
   A. *“Receiv[ing]. . . An Indication [and] a Network Address”*

3. **Dependent Claims**

   A. *“email” and “secure domain name”*

The Challenged Claims:

“audio/video data”



US0085

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

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

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,958**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0117237 A1 May 10, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **Referen**

U.S. PATENT

2,895,502 A 7/1959
4,677,434 A 6/1987

(Con

FOREIGN PATE

DE 19924575
EP 0838930

(Con

OTHER PU

U.S. Appl. No. 09/399,753, filed

(Con

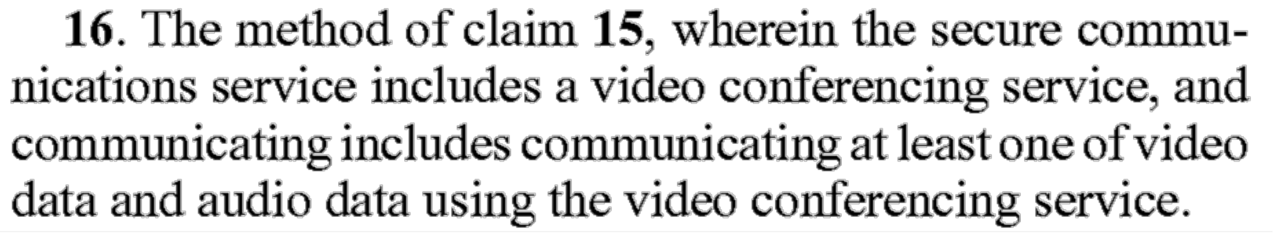
Primary Examiner — Krisna
(74) *Attorney, Agent, or Fir*
LLP

(57) **ABS**

A network device comprises a
cation program for a secure
least one processor configure
gram enabling the network
look up a network address of
on an identifier; (b) receive
network device is available
service, the indication including the requested network address of the second network device and provisioning information for a secure communication link; (c) connect to the second network device over the secure communication link, using the received network address of the second network device and the provisioning information for the secure communication link; and (d) co
data and audio data with the s
secure communications serv
tion link.

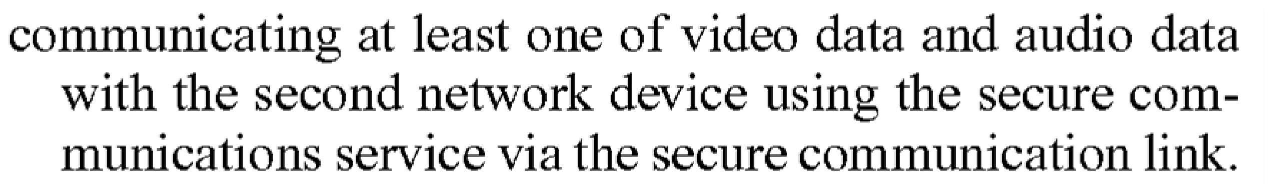
27 Claims, 40

Petitioner A



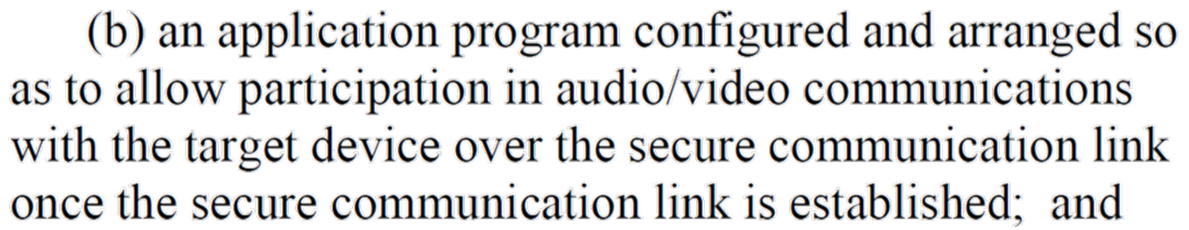
16. The method of claim **15**, wherein the secure communications service includes a video conferencing service, and communicating includes communicating at least one of video data and audio data using the video conferencing service.

’341 Patent (Ex. 1001) at Claim 1



communicating at least one of video data and audio data with the second network device using the secure communications service via the secure communication link.

’131 Patent (Ex. 1003) at Claim 1

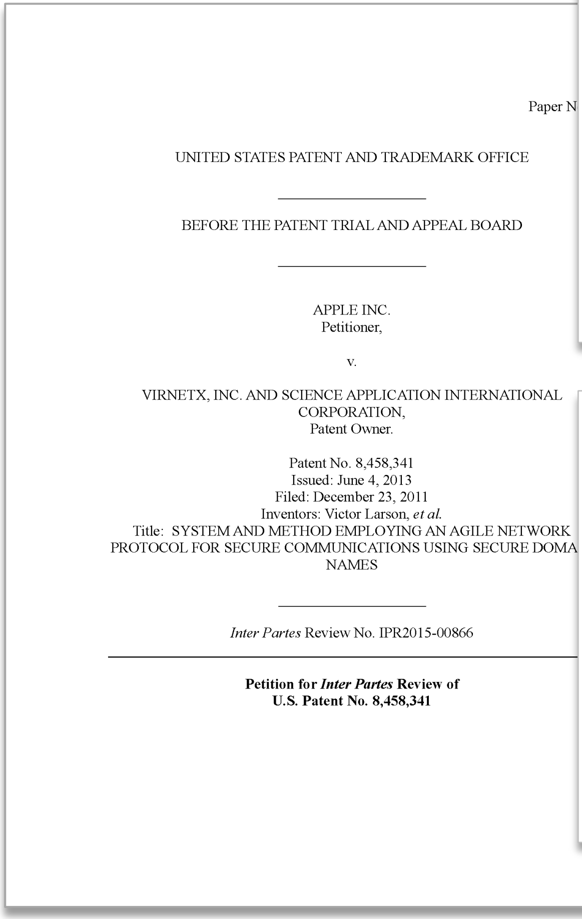


(b) an application program configured and arranged so as to allow participation in audio/video communications with the target device over the secure communication link once the secure communication link is established; and

’705 Patent (Ex. 1050) at Claim 1

Combining Beser and RFC 2401

“audio/video data”



Paper N

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

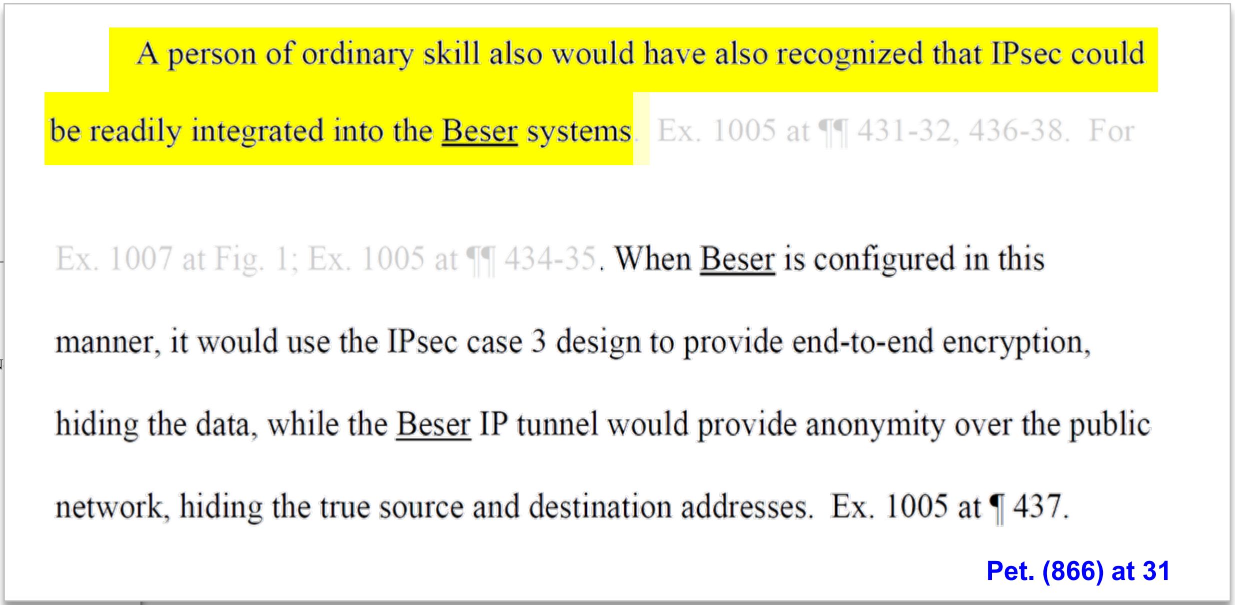
v.

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

Patent No. 8,458,341
Issued: June 4, 2013
Filed: December 23, 2011
Inventors: Victor Larson, *et al.*
Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK
PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMA
NAMES

Inter Partes Review No. IPR2015-00866

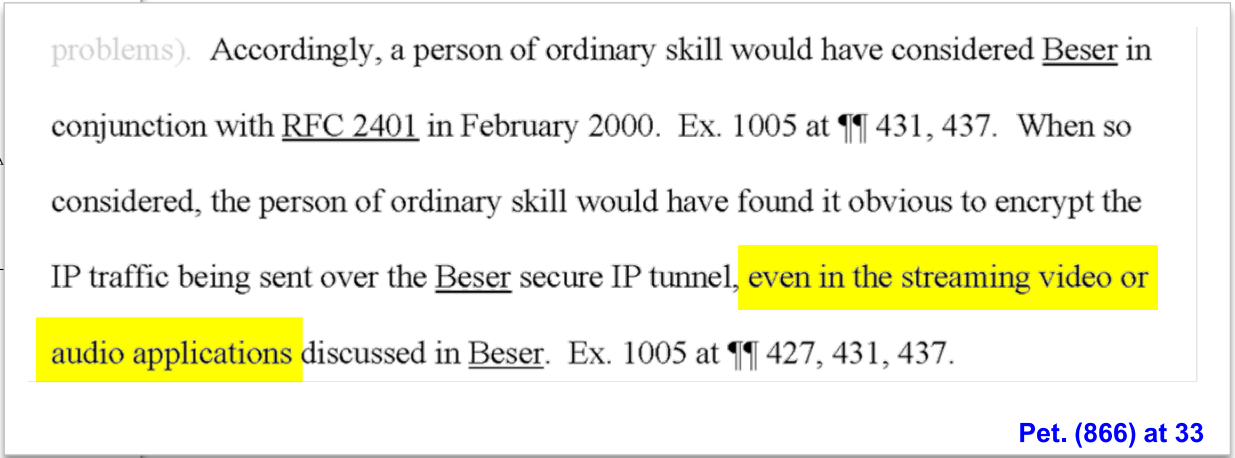
Petition for *Inter Partes* Review of
U.S. Patent No. 8,458,341



A person of ordinary skill also would have also recognized that IPsec could be readily integrated into the Beser systems. Ex. 1005 at ¶¶ 431-32, 436-38. For

Ex. 1007 at Fig. 1; Ex. 1005 at ¶¶ 434-35. 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 ¶ 437.

Pet. (866) at 31

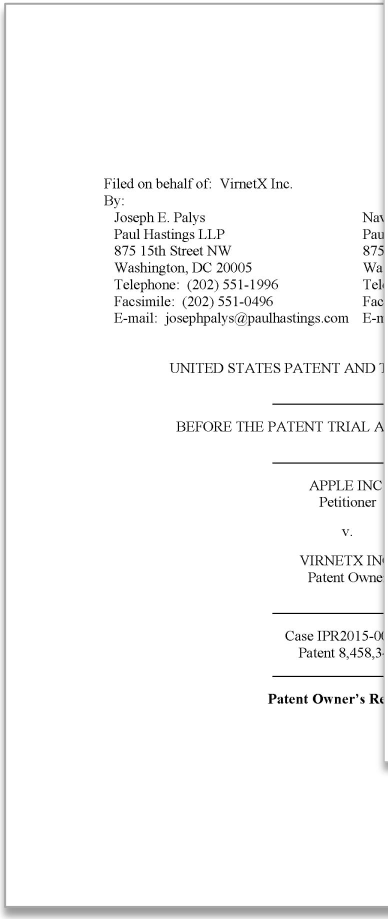


problems). Accordingly, a person of ordinary skill would have considered Beser in conjunction with RFC 2401 in February 2000. Ex. 1005 at ¶¶ 431, 437. When so considered, the person of ordinary skill would have found it obvious to encrypt the IP traffic being sent over the Beser secure IP tunnel, even in the streaming video or audio applications discussed in Beser. Ex. 1005 at ¶¶ 427, 431, 437.

Pet. (866) at 33

Patent Owner Assertion

Combining Beser and RFC 2401



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

Nav
Pau
875
Wa
Tel
Fac
E-n

UNITED STATES PATENT AND T

BEFORE THE PATENT TRIAL A

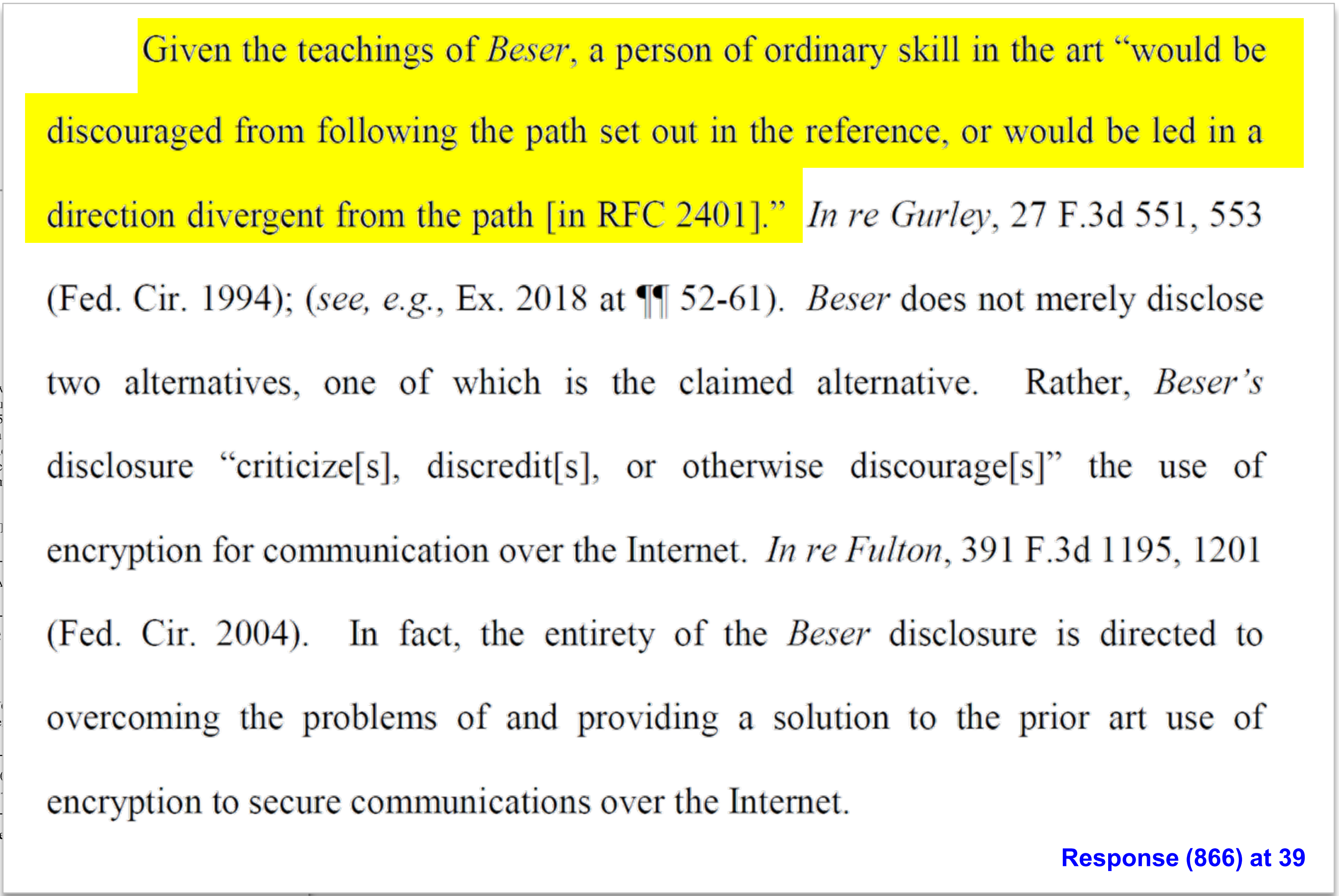
APPLE INC
Petitioner

v.

VIRNETX IN
Patent Owne

Case IPR2015-0
Patent 8,458,3

Patent Owner's Re

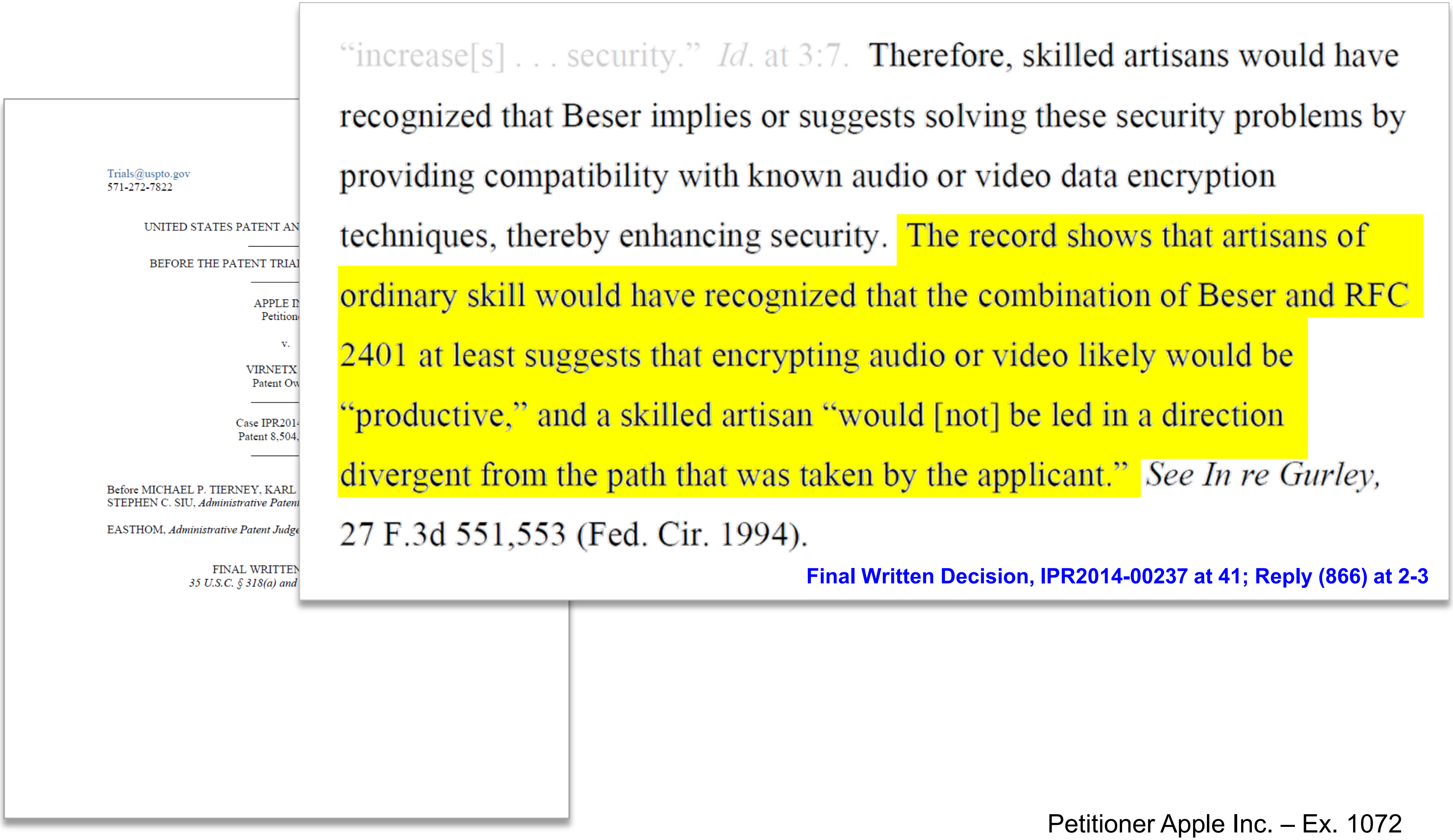


Given the teachings of *Beser*, a person of ordinary skill in the art "would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path [in RFC 2401]." *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994); (*see, e.g.*, Ex. 2018 at ¶¶ 52-61). *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.

Response (866) at 39

Final Written Decision in IPR2014-00237

Combining Beser and RFC 2401



Trials@uspto.gov
571-272-7822

UNITED STATES PATENT AN

BEFORE THE PATENT TRIAI

APPLE I
Petition

v.

VIRNETX
Patent Ow

Case IPR201
Patent 8,504,

Before MICHAEL P. TIERNEY, KARL
STEPHEN C. SIU, *Administrative Patent*

EASTHOM, *Administrative Patent Judge*

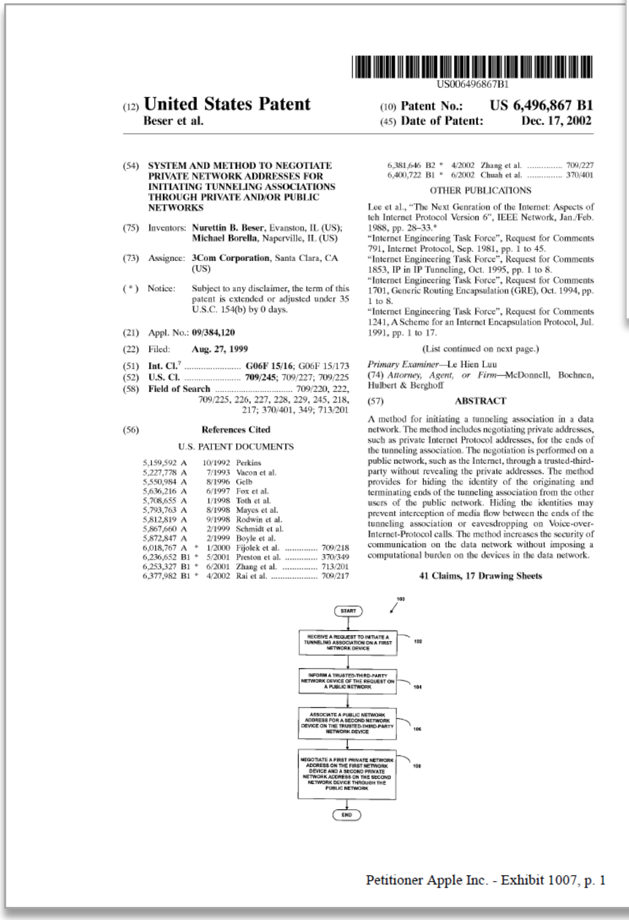
FINAL WRITTEN
35 U.S.C. § 318(a) and

"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 (866) at 2-3

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

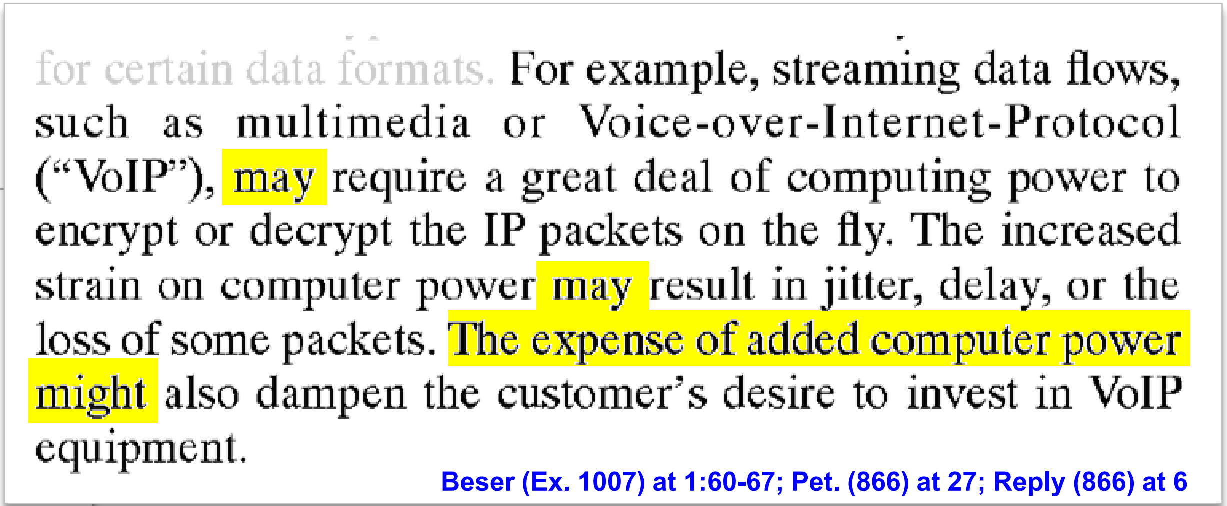
(57) **ABSTRACT**

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

100
START
RECEIVE A REQUEST TO INITIATE A TUNNELING ASSOCIATION ON A FIRST NETWORK DEVICE
102
INFORM A TRUSTED-THIRD-PARTY NETWORK DEVICE OF THE REQUEST ON A PUBLIC NETWORK
104
ASSOCIATE A PUBLIC NETWORK ADDRESS FOR A SECOND NETWORK DEVICE ON THE TRUSTED-THIRD-PARTY NETWORK DEVICE
106
NEGOTIATE A FIRST PRIVATE NETWORK ADDRESS ON THE FIRST NETWORK DEVICE AND A SECOND PRIVATE NETWORK ADDRESS ON THE SECOND NETWORK DEVICE THROUGH THE PUBLIC NETWORK
108
END

Petitioner Apple Inc. - Exhibit 1007, p. 1

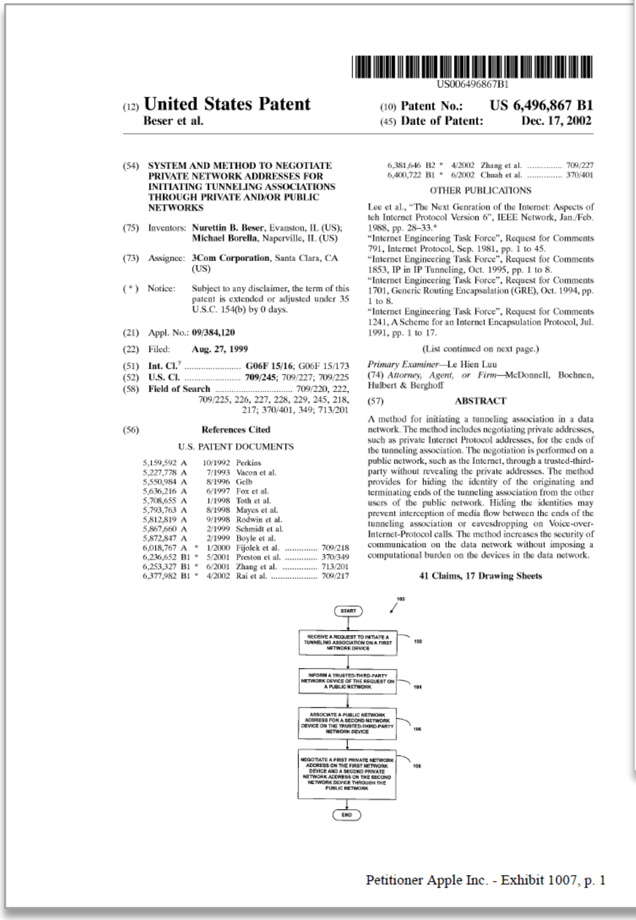


for certain data formats. For example, streaming data flows, such as multimedia or Voice-over-Internet-Protocol ("VoIP"), may require a great deal of computing power to encrypt or decrypt the IP packets on the fly. The increased strain on computer power may result in jitter, delay, or the loss of some 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. (866) at 27; Reply (866) at 6

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

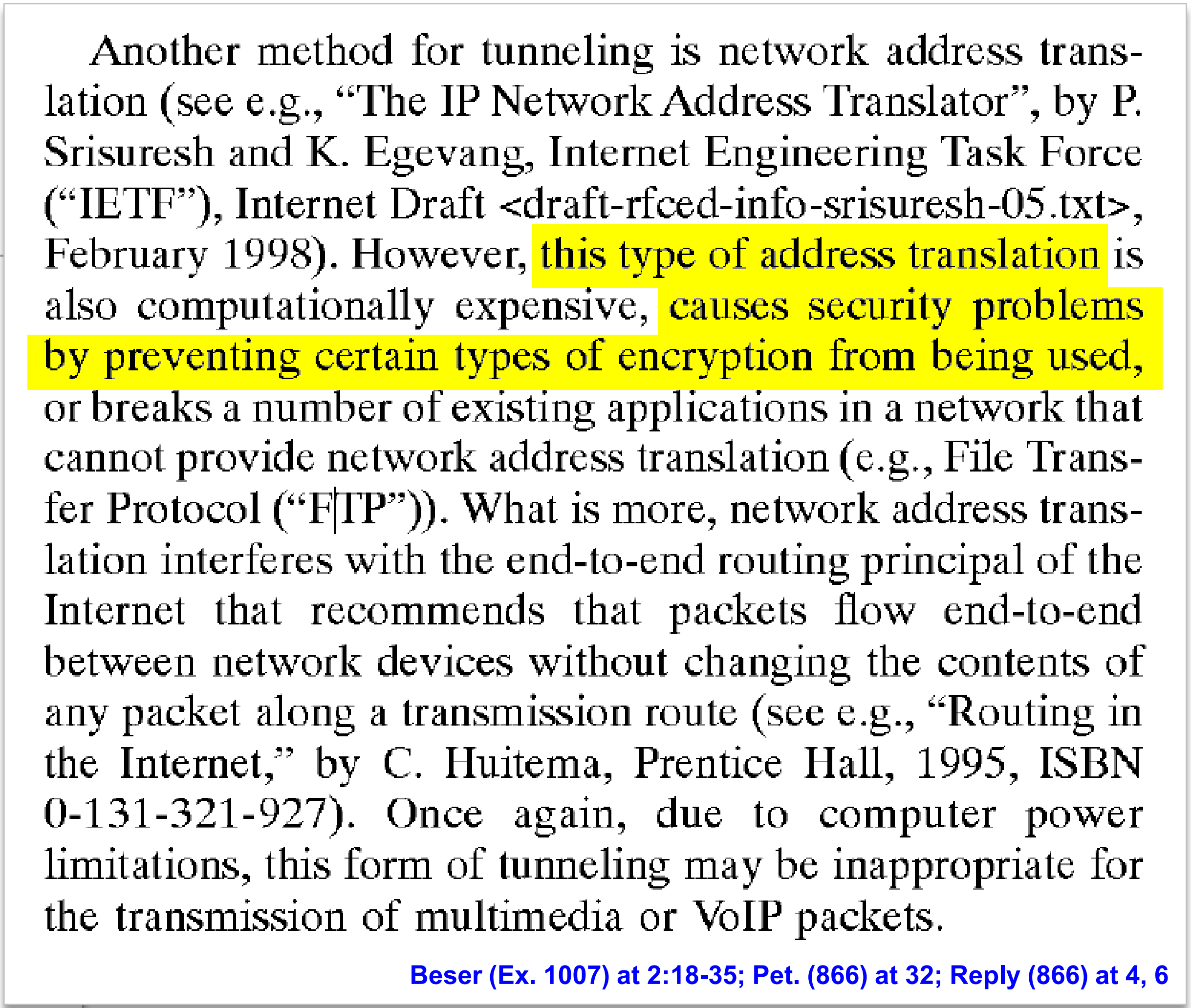
(57) **ABSTRACT**

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

100
START
RECEIVE A REQUEST TO INITIATE A TUNNELING ASSOCIATION ON A FIRST NETWORK DEVICE
102
INFORM A TRUSTED-THIRD-PARTY NETWORK DEVICE OF THE REQUEST ON A PUBLIC NETWORK
104
ASSOCIATE A PUBLIC NETWORK ADDRESS FOR A SECOND NETWORK DEVICE ON THE TRUSTED-THIRD-PARTY NETWORK DEVICE
106
NEGOTIATE A FIRST PRIVATE NETWORK ADDRESS ON THE FIRST NETWORK DEVICE AND A SECOND PRIVATE NETWORK ADDRESS ON THE SECOND NETWORK DEVICE THROUGH THE PUBLIC NETWORK
108
END

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. (866) at 32; Reply (866) at 4, 6

IPR2015-00866, -868, -870

Beser and RFC 2401 Issues

1. **Common Issues (866, 868, & 870)**

   A. "Virtual Private Network Communication Link" (866: claims; 868: claim 10; 870: claims 6 & 21)

   B. Encrypting audio/visual data

   C. Combining Beser and RFC 2401 would have been obvious

   D. A "*request to look up an []IP address… based on a domain name associated with the second network [target] device*"

   E. "*Interception of the request to look up an Internet Protocol (IP) address*"

2. **Issues Affecting 866 & 868 Only**

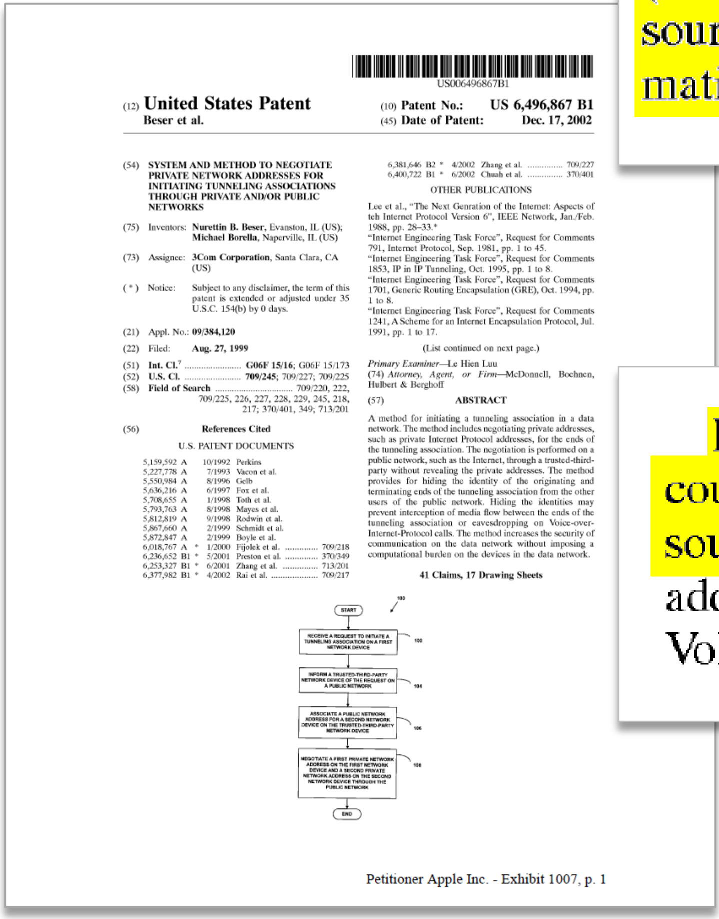
   A. "Receiv[ing]. . . An Indication [and] a Network Address"

3. **Dependent Claims**

   A. "email" and "secure domain name"

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

100
START
RECEIVE A REQUEST TO INITIATE A TUNNELING ASSOCIATION ON A FIRST NETWORK DEVICE
102
INFORM A TRUSTED-THIRD-PARTY NETWORK DEVICE OF THE REQUEST ON A PUBLIC NETWORK
104
ASSOCIATE A PUBLIC NETWORK ADDRESS FOR A SECOND NETWORK DEVICE ON THE TRUSTED-THIRD-PARTY NETWORK DEVICE
106
NEGOTIATE A FIRST PRIVATE NETWORK ADDRESS ON THE FIRST NETWORK DEVICE AND A SECOND PRIVATE NETWORK ADDRESS ON THE SECOND NETWORK DEVICE THROUGH THE PUBLIC NETWORK
108
END

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. (866) at 27, 29-31

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.

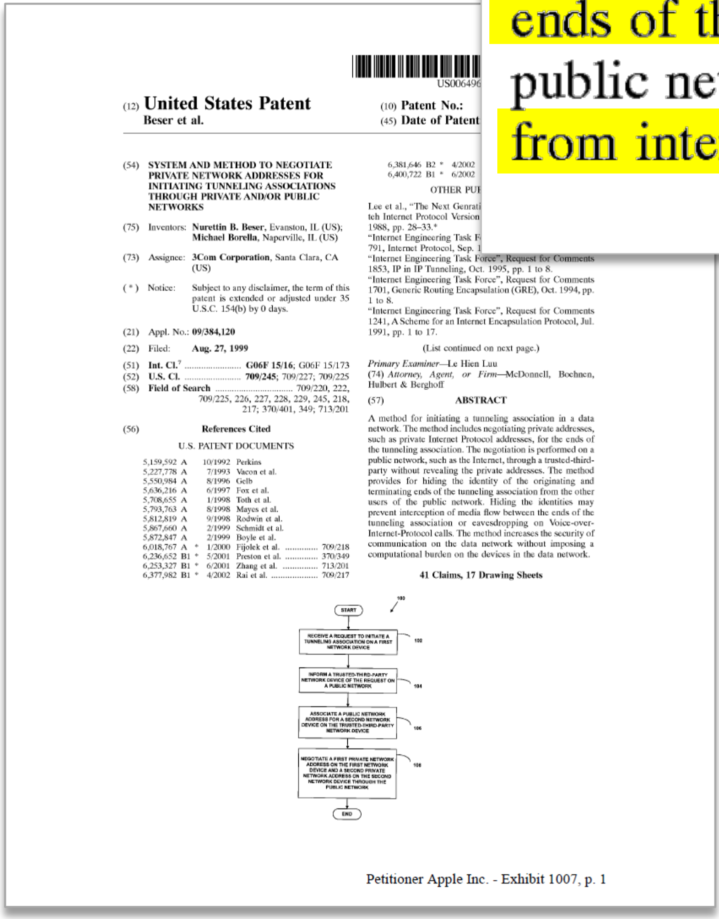
Beser (Ex. 1007) at 2:1-5; Reply (866) at 4

Beser and RFC 2401

Combining Beser and RFC 2401

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 (866) at 5



US006496

(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
6,381,646	B2	*	4/2002		
6,400,722	B1	*	6/2002		

OTHER PUI

Lee et al., "The Next Genrati
teh Internet Protocol Version
1988, pp. 28–33.*
"Internet Engineering Task F
791, Internet Protocol, Sep. 1
"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

100
START
RECEIVE A REQUEST TO INITIATE A TUNNELING ASSOCIATION ON A FIRST NETWORK DEVICE
102
INFORM A TRUSTED-THIRD-PARTY NETWORK DEVICE OF THE REQUEST ON A PUBLIC NETWORK
104
ASSOCIATE A PUBLIC NETWORK ADDRESS FOR A SECOND NETWORK DEVICE ON THE TRUSTED-THIRD-PARTY NETWORK DEVICE
106
NEGOTIATE A FIRST PRIVATE NETWORK ADDRESS ON THE FIRST NETWORK DEVICE AND A SECOND PRIVATE NETWORK ADDRESS ON THE SECOND NETWORK DEVICE THROUGH THE PUBLIC NETWORK
108
END

Petitioner Apple Inc. - Exhibit 1007, p. 1

IPR2015-00866, -868, -870

Beser and RFC 2401 Issues

1. **Common Issues (866, 868, & 870)**

   A. "Virtual Private Network Communication Link" (866: claims; 868: claim 10; 870: claims 6 & 21)

   B. Encrypting audio/visual data

   C. Combining Beser and RFC 2401 would have been obvious

   D. A "*request to look up an []IP address… based on a domain name associated with the second network [target] device*"

   E. "*Interception of the request to look up an Internet Protocol (IP) address*"

2. **Issues Affecting 866 & 868 Only**

   A. "Receiv[ing]. . . An Indication [and] a Network Address"

3. **Dependent Claims**

   A. "email" and "secure domain name"

The Challenged Claims:

“a request to look up an Internet Protocol (IP) address… based on a domain name”

sending a request to look up an internet protocol (IP) address of a second network device based on a domain name associated with the second network device;

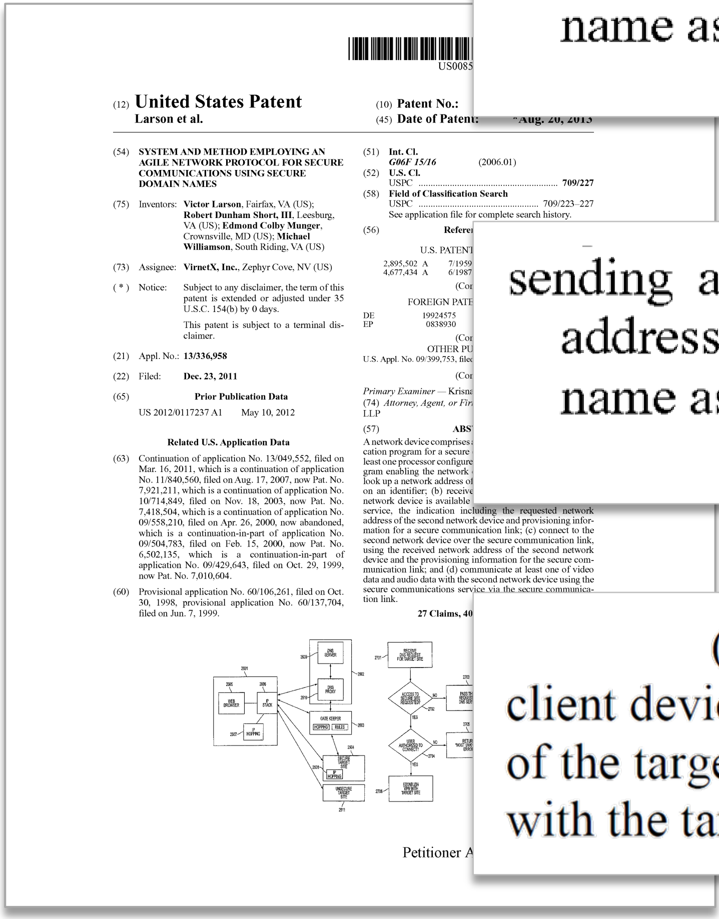
’341 Patent (Ex. 1001) at Claim 15

sending a request to look up an internet protocol (IP) address of a second network device based on a domain name associated with the second network device;

’131 Patent (Ex. 1003) at Claim 15

(i) interception of a request, generated by the client device, to look up an internet protocol (IP) address of the target device based on a domain name associated with the target device, and

’705 Patent (Ex. 1050) at Claim 1



US0085

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

(10) **Patent No.:**
(45) **Date of Patent:** *Aug. 20, 2013

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,958**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0117237 A1 May 10, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **Referen**

U.S. PATENT

2,895,502 A 7/1959
4,677,434 A 6/1987

(Con

FOREIGN PATE

DE 19924575
EP 0838930

(Con

OTHER PU

U.S. Appl. No. 09/399,753, filed

(Con

Primary Examiner — Krisna
(74) *Attorney, Agent, or Fir*
LLP

(57) **ABS**

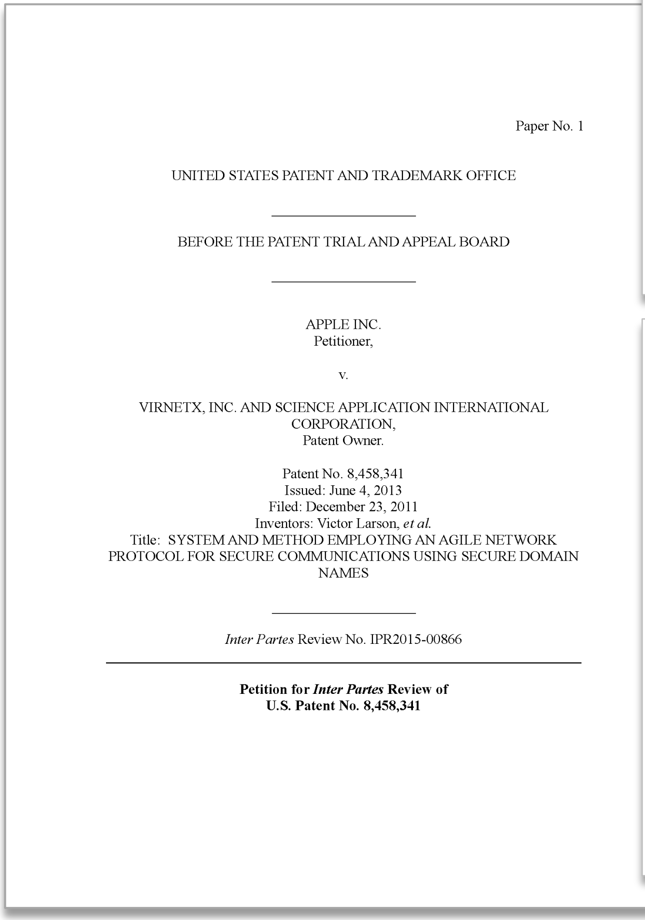
A network device comprises a cation program for a secure least one processor configure gram enabling the network look up a network address of on an identifier; (b) receive network device is available service, the indication including the requested network address of the second network device and provisioning information for a secure communication link; (c) connect to the second network device over the secure communication link, using the received network address of the second network device and the provisioning information for the secure communication link; and (d) communicate at least one of video data and audio data with the second network device using the secure communications service via the secure communication link.

27 Claims, 40

Petitioner A

Beser and RFC 2401

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



Paper No. 1

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

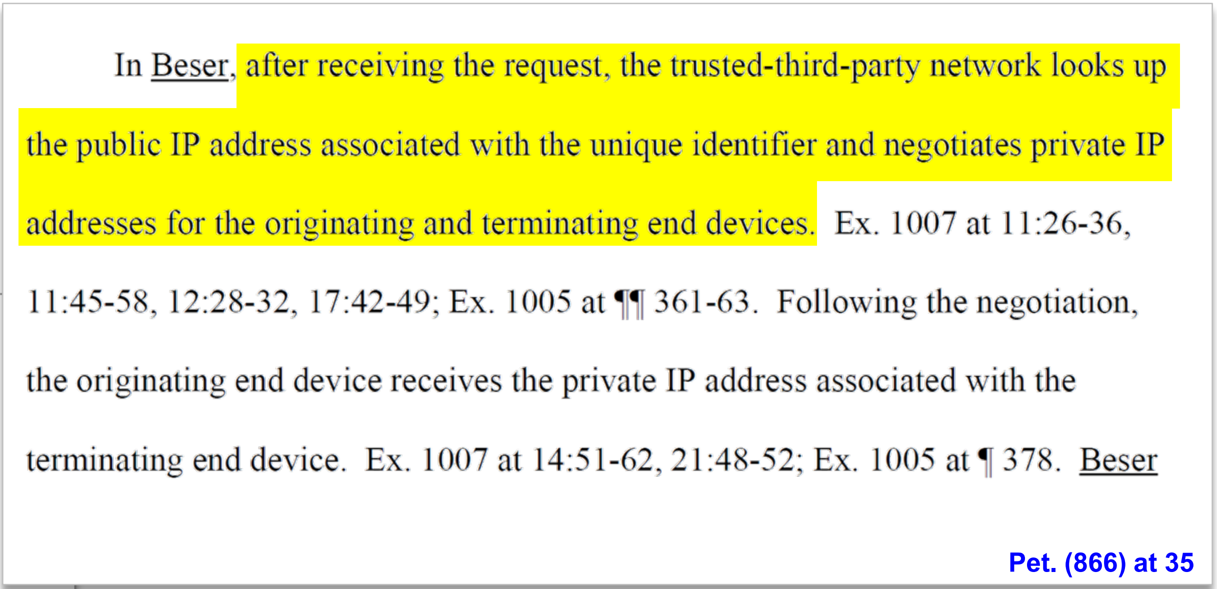
v.

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

Patent No. 8,458,341
Issued: June 4, 2013
Filed: December 23, 2011
Inventors: Victor Larson, *et al.*
Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

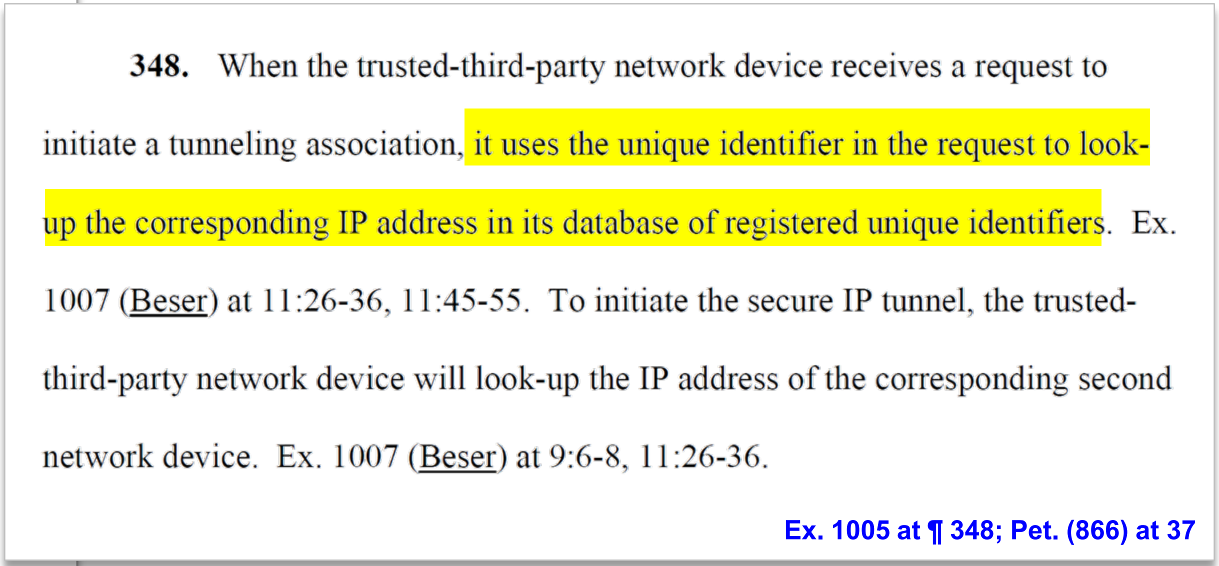
Inter Partes Review No. IPR2015-00866

Petition for *Inter Partes* Review of
U.S. Patent No. 8,458,341



In Beser, after receiving the request, the trusted-third-party network looks up the public IP address associated with the unique identifier and negotiates private IP addresses for the originating and terminating end devices. Ex. 1007 at 11:26-36, 11:45-58, 12:28-32, 17:42-49; Ex. 1005 at ¶¶ 361-63. Following the negotiation, the originating end device receives the private IP address associated with the terminating end device. Ex. 1007 at 14:51-62, 21:48-52; Ex. 1005 at ¶ 378. Beser

Pet. (866) at 35

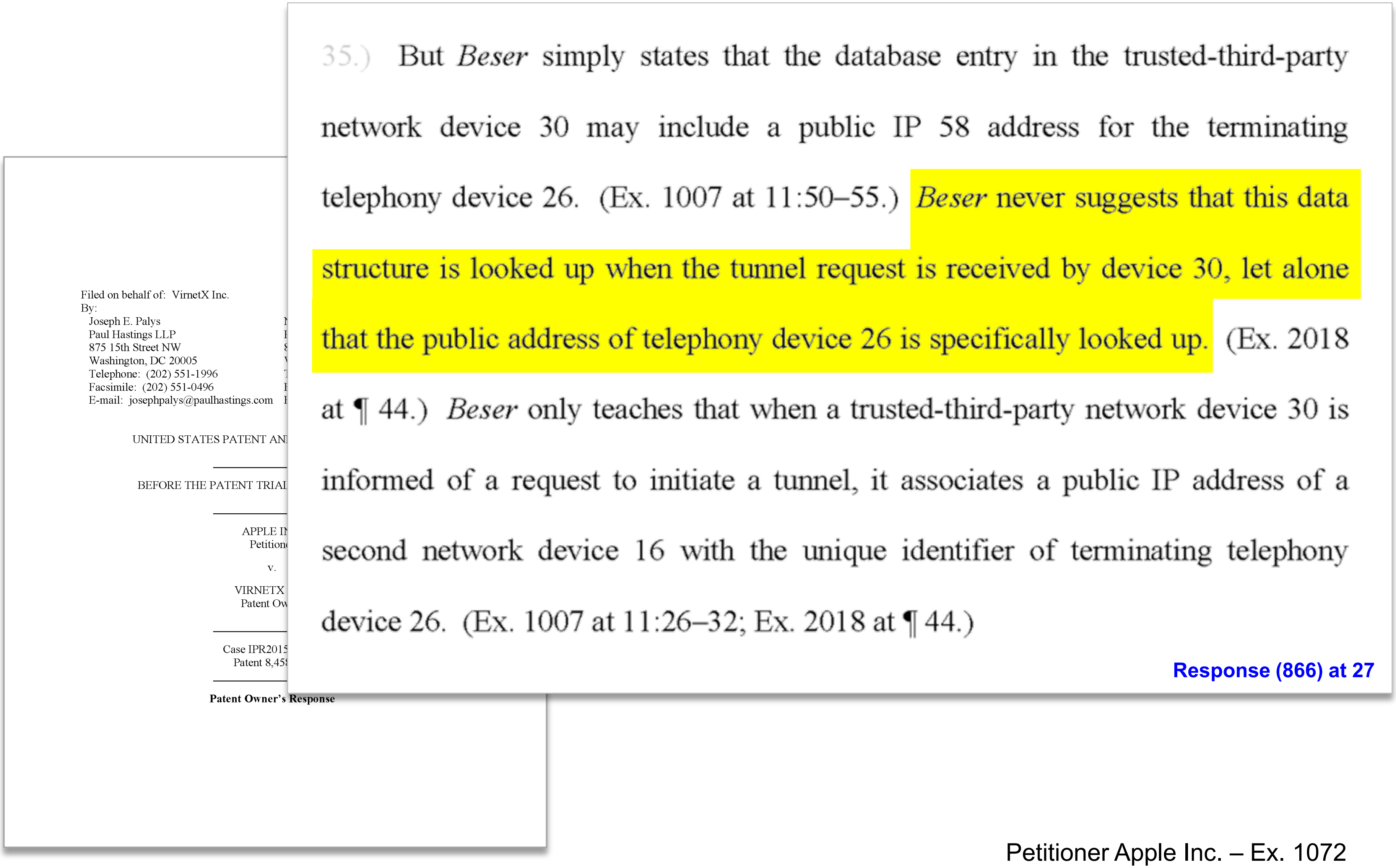


348. When the trusted-third-party network device receives a request to initiate a tunneling association, it uses the unique identifier in the request to look-up the corresponding IP address in its database of registered unique identifiers. Ex. 1007 (Beser) at 11:26-36, 11:45-55. To initiate the secure 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 ¶ 348; Pet. (866) at 37

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

UNITED STATES PATENT AN

BEFORE THE PATENT TRIAL

APPLE I
Petition

v.

VIRNETX
Patent Ow

Case IPR2015
Patent 8,45

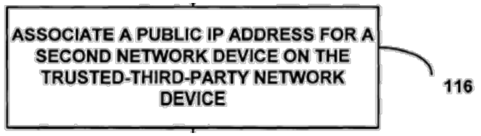
Patent Owner's Response

35.) 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. (Ex. 2018 at ¶ 44.) *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. 2018 at ¶ 44.)

Response (866) at 27

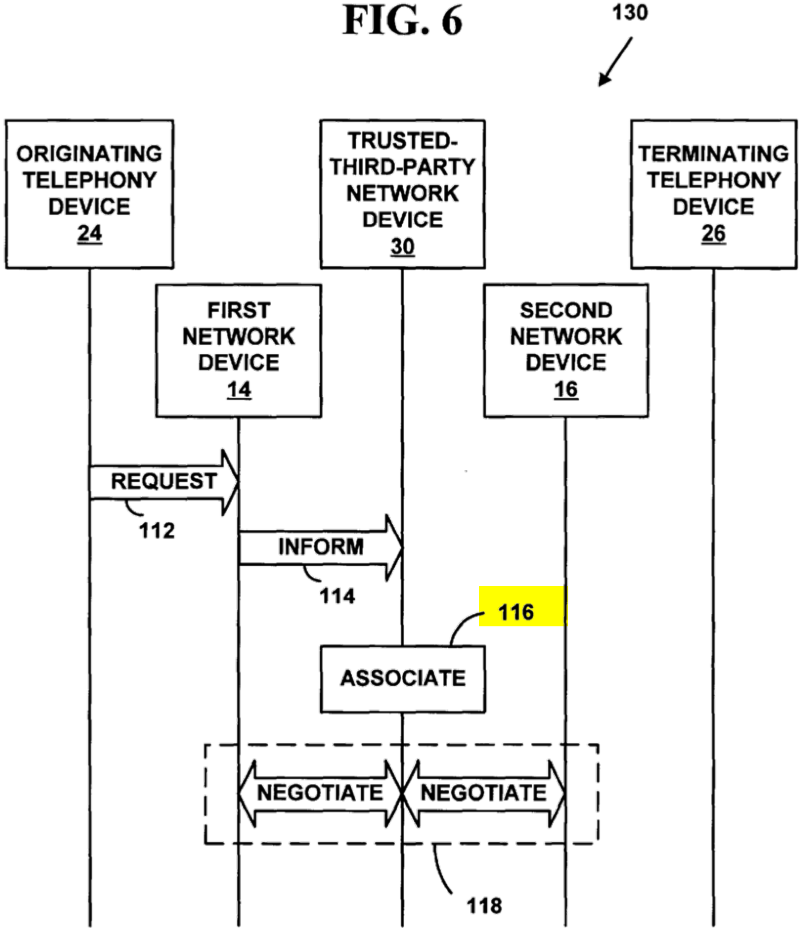
Beser and RFC 2401

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

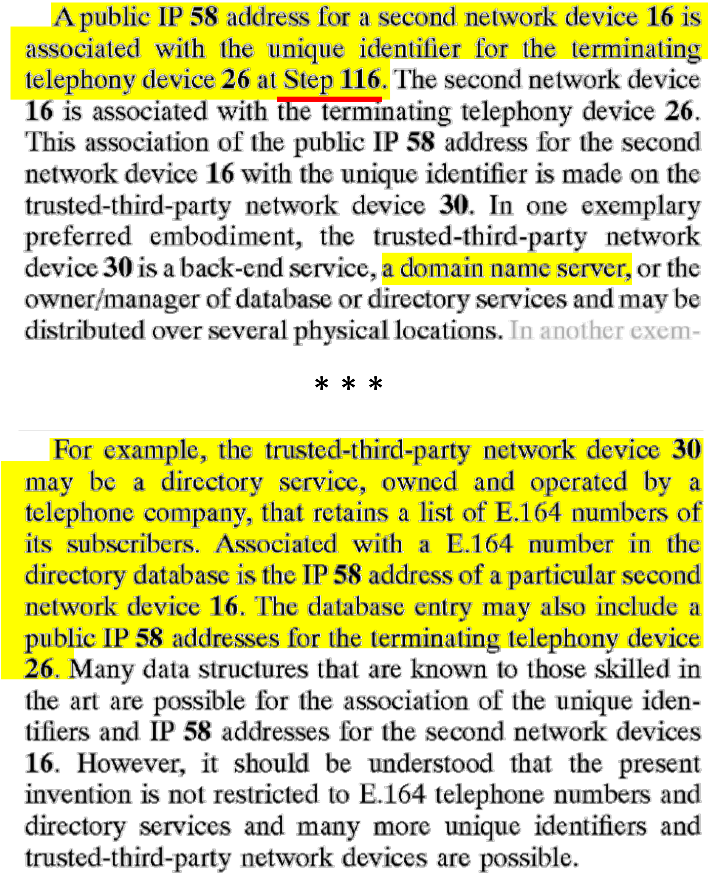

ASSOCIATE A PUBLIC IP ADDRESS FOR A SECOND NETWORK DEVICE ON THE TRUSTED-THIRD-PARTY NETWORK DEVICE
116

Beser (Ex. 1007) at Fig. 5; Reply (866) at 9-10

FIG. 6



Beser (Ex. 1007) at Fig. 6; Pet. (866) at 19-21, 38



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-

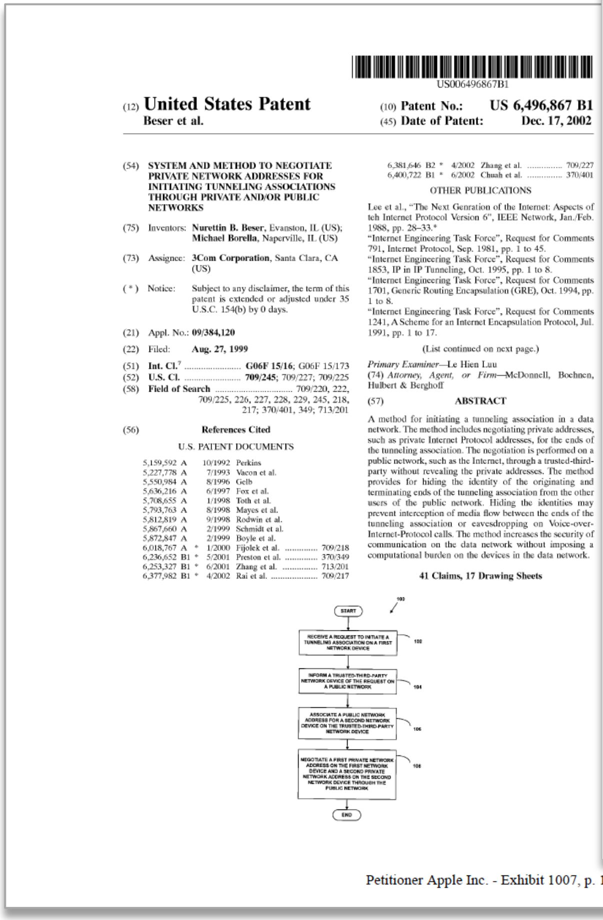
* * *

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. (866) at 38

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**

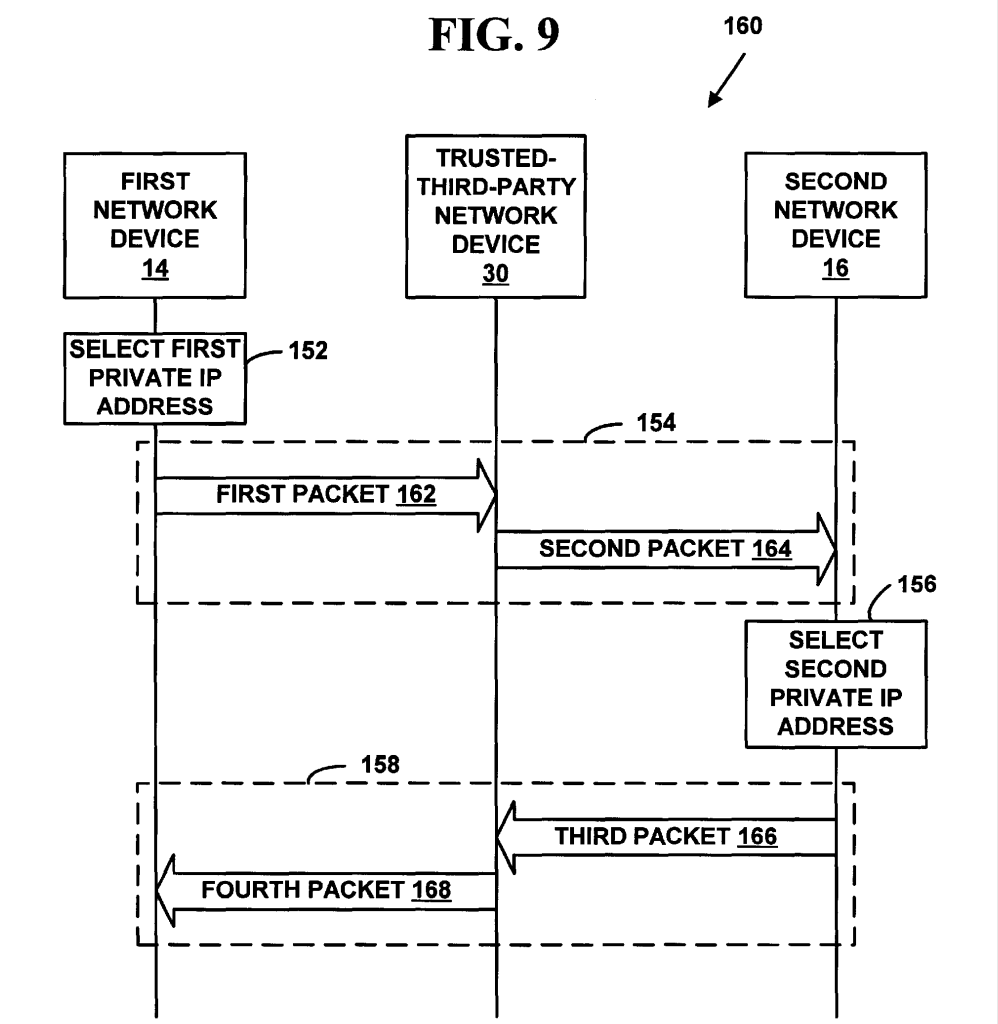
A method for initiating a tunneling association in a data network. The method includes negotiating private addresses, such as private Internet Protocol addresses, for the ends of the tunneling association. The negotiation is performed on a public network, such as the Internet, through a trusted-third-party 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

100
START
RECEIVE A REQUEST TO INITIATE A TUNNELING ASSOCIATION ON A FIRST NETWORK DEVICE
102
INFORM A TRUSTED-THIRD-PARTY NETWORK DEVICE OF THE REQUEST ON A PUBLIC NETWORK
104
ASSOCIATE A PUBLIC NETWORK ADDRESS FOR A SECOND NETWORK DEVICE ON THE TRUSTED-THIRD-PARTY NETWORK DEVICE
106
NEGOTIATE A FIRST PRIVATE NETWORK ADDRESS ON THE FIRST NETWORK DEVICE AND A SECOND PRIVATE NETWORK ADDRESS ON THE SECOND NETWORK DEVICE THROUGH THE PUBLIC NETWORK
108
END

Petitioner Apple Inc. - Exhibit 1007, p. 1

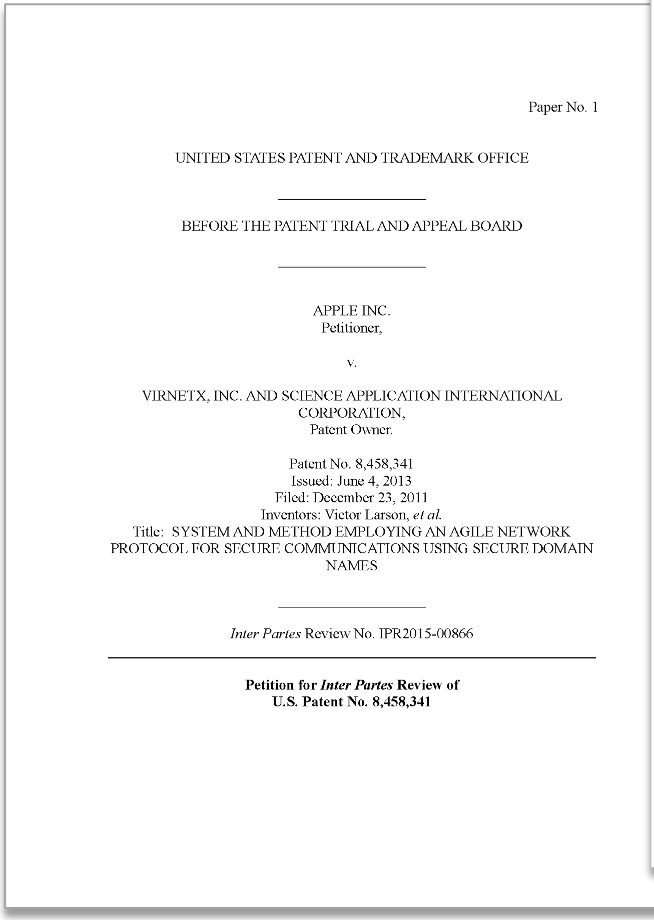
FIG. 9



Beser (Ex. 1007) at Fig. 9; Pet. (866) at 22-23

Beser and RFC 2401

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



Paper No. 1

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

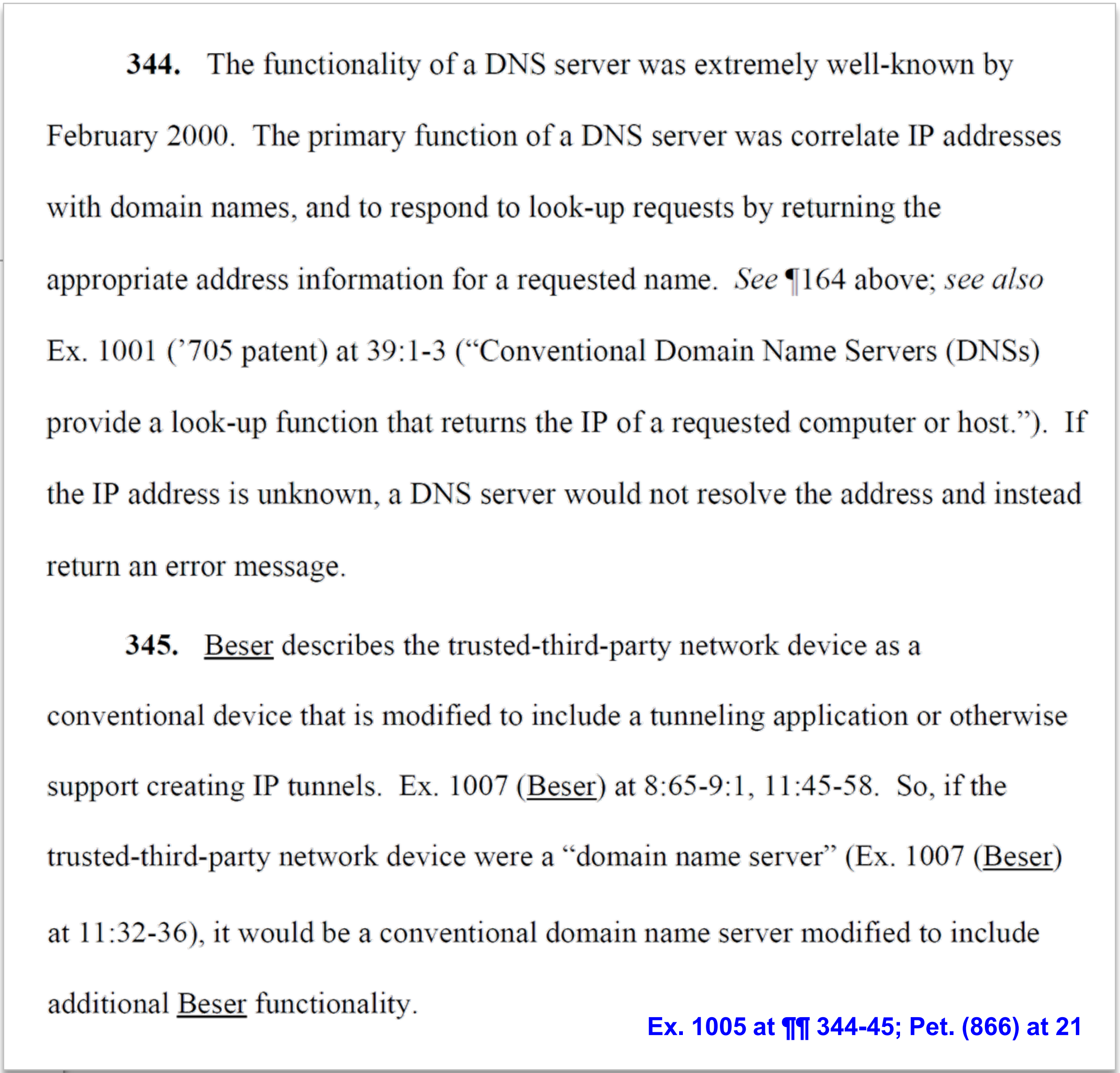
v.

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

Patent No. 8,458,341
Issued: June 4, 2013
Filed: December 23, 2011
Inventors: Victor Larson, *et al.*
Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Inter Partes Review No. IPR2015-00866

Petition for *Inter Partes* Review of
U.S. Patent No. 8,458,341



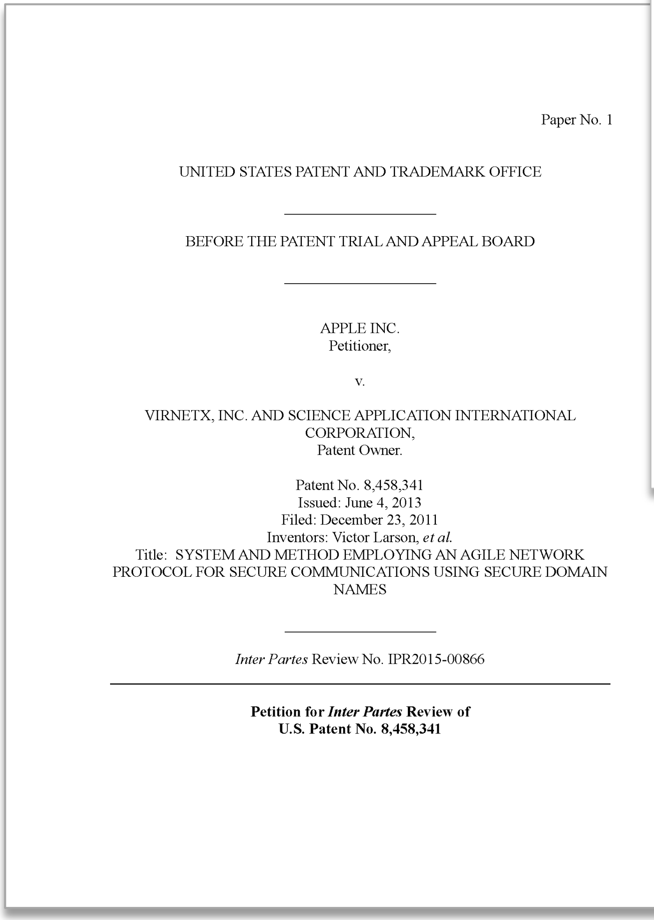
344. The functionality of a DNS server was extremely well-known by February 2000. The primary function of a DNS server was correlate IP addresses with domain names, and to respond to look-up requests by returning the appropriate address information for a requested name. *See* ¶164 above; *see also* Ex. 1001 ('705 patent) at 39:1-3 ("Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP of a requested computer or host."). If the IP address is unknown, a DNS server would not resolve the address and instead return an error message.

345. Beser describes the trusted-third-party network device as a conventional device that is modified to include a tunneling application or otherwise support creating IP tunnels. Ex. 1007 (Beser) at 8:65-9:1, 11:45-58. So, if the trusted-third-party network device were a "domain name server" (Ex. 1007 (Beser) at 11:32-36), it would be a conventional domain name server modified to include additional Beser functionality.

Ex. 1005 at ¶¶ 344-45; Pet. (866) at 21

Beser and RFC 2401

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



Paper No. 1

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

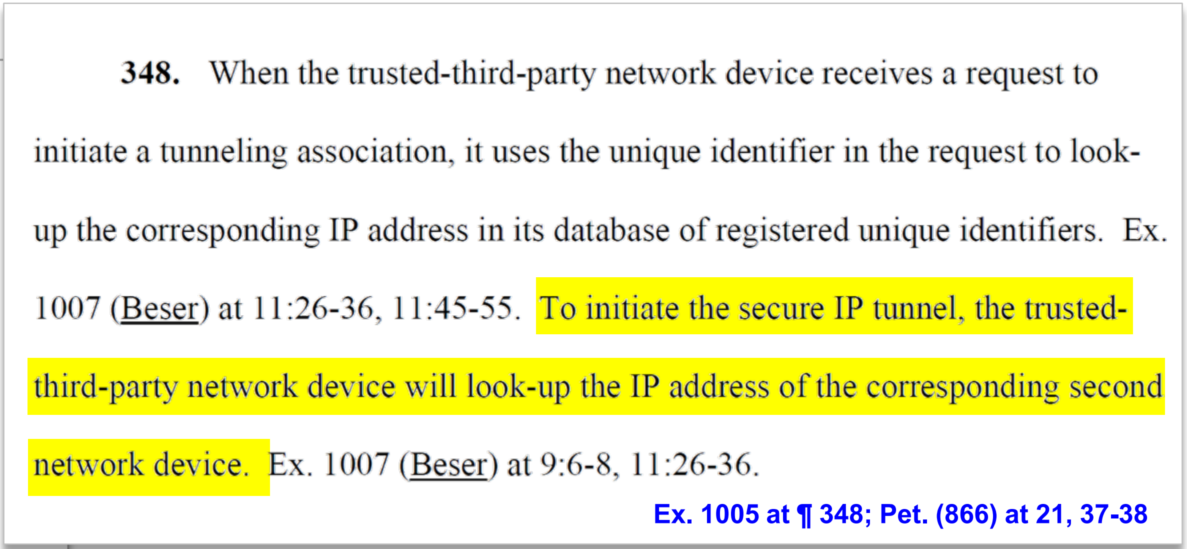
v.

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

Patent No. 8,458,341
Issued: June 4, 2013
Filed: December 23, 2011
Inventors: Victor Larson, *et al.*
Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK
PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN
NAMES

Inter Partes Review No. IPR2015-00866

**Petition for *Inter Partes* Review of
U.S. Patent No. 8,458,341**



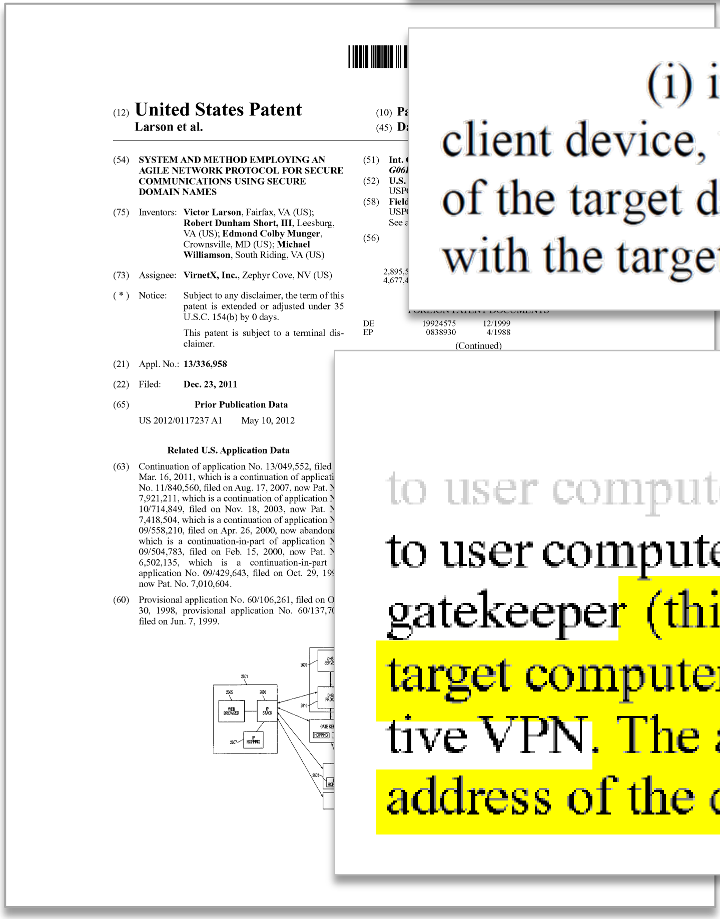
348. When the trusted-third-party network device receives a request to initiate a tunneling association, it uses the unique identifier in the request to look-up the corresponding IP address in its database of registered unique identifiers. Ex. 1007 (Beser) at 11:26-36, 11:45-55. To initiate the secure 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 ¶ 348; Pet. (866) at 21, 37-38

The Challenged Claims vs. the Specification:
“a request to look up an Internet Protocol (IP) address”

sending a request to look up an internet protocol (IP) address of a second network device based on a domain name associated with the second network device;

’341 Patent (Ex. 1001) at Claim 15; ’131 Patent (Ex. 1003) at Claim 15



(12) United States Patent
Larson et al.

(10) Pa
(45) D

(54) SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,958**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0117237 A1 May 10, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed Mar. 16, 2011, which is a continuation of applicati No. 11/840,560, filed on Aug. 17, 2007, now Pat. N 7,921,211, which is a continuation of application N 10/714,849, filed on Nov. 18, 2003, now Pat. N 7,418,504, which is a continuation of application N 09/558,210, filed on Apr. 26, 2000, now abandon which is a continuation-in-part of application N 09/504,783, filed on Feb. 15, 2000, now Pat. N 6,502,135, which is a continuation-in-part application No. 09/429,643, filed on Oct. 29, 19 now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on O 30, 1998, provisional application No. 60/137,7 filed on Jun. 7, 1999.

(51) Int. (
G06
(52) U.S.
USP(
(58) Field
USP(
See a
(56)

2,895,5
4,677,4

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

(i) interception of a request, generated by the client device, to look up an internet protocol (IP) address of the target device based on a domain name associated with the target device, and

’705 Patent (Ex. 1050) at Claim 1

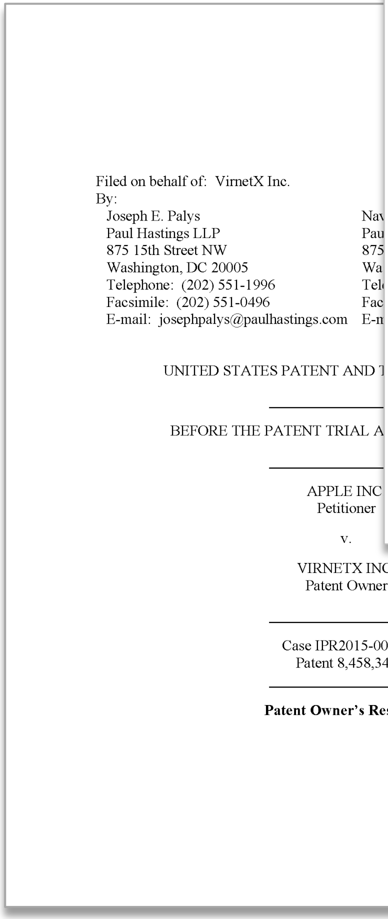
Patent Owner’s Specification

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.

’341 Patent (Ex. 1001) at 40:39-44

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

Nav
Pau
875
Wa
Tel
Fac
E-m

UNITED STATES PATENT AND T

BEFORE THE PATENT TRIAL A

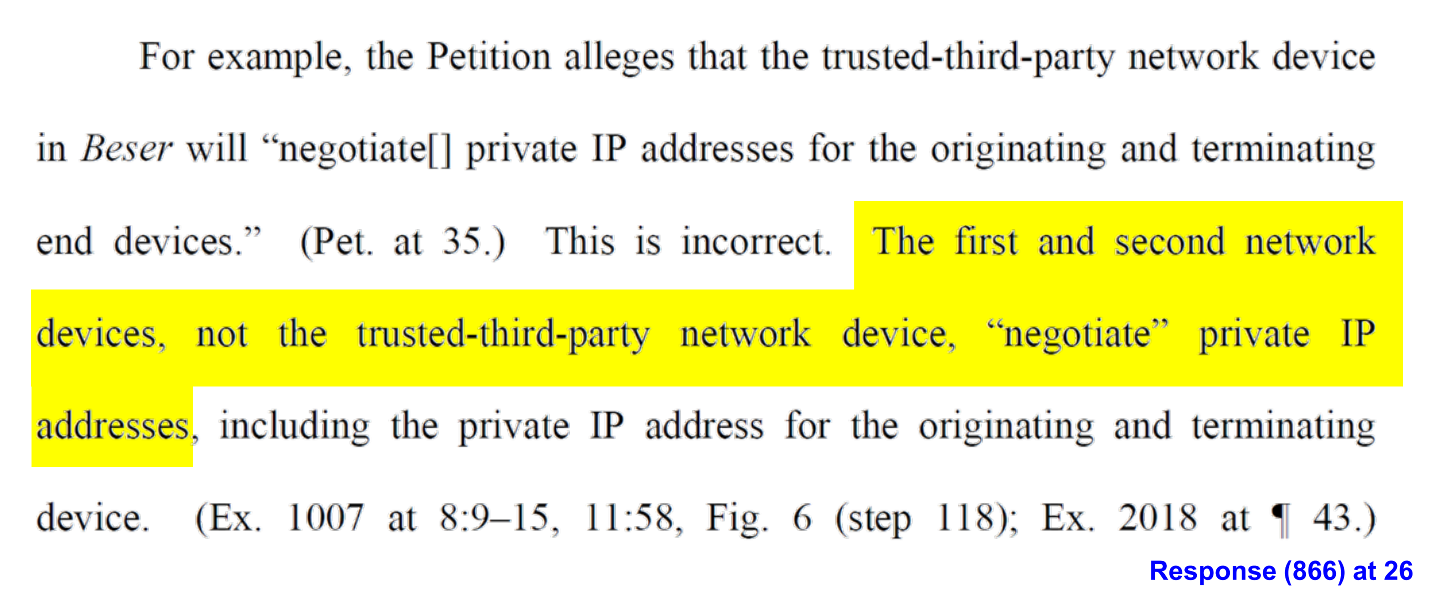
APPLE INC
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2015-00866
Patent 8,458,341

Patent Owner's Response



For example, the Petition alleges that the trusted-third-party network device in *Beser* will "negotiate[] private IP addresses for the originating and terminating end devices." (Pet. at 35.) 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 originating and terminating device. (Ex. 1007 at 8:9–15, 11:58, Fig. 6 (step 118); Ex. 2018 at ¶ 43.)

Response (866) at 26

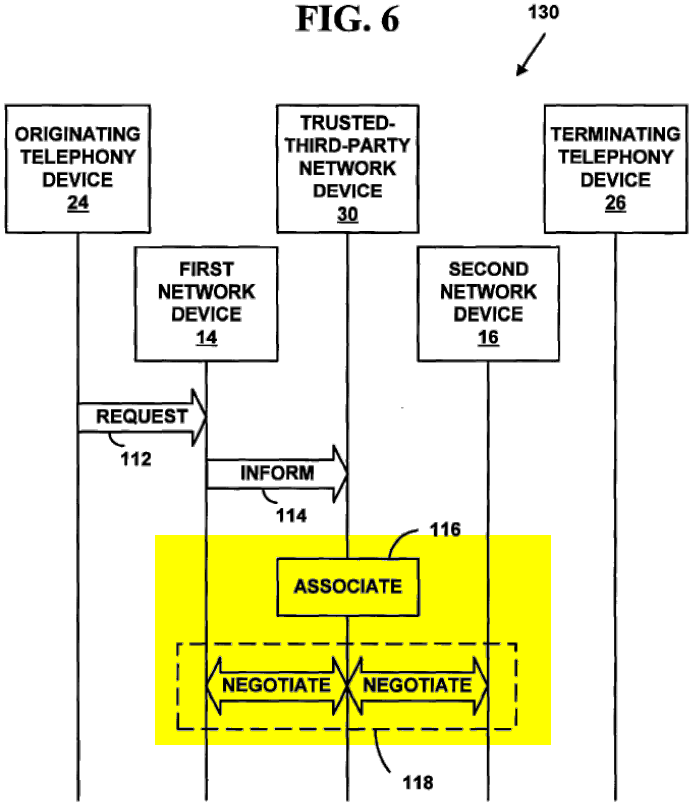
Grounds Based on Beser and RFC 2401

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

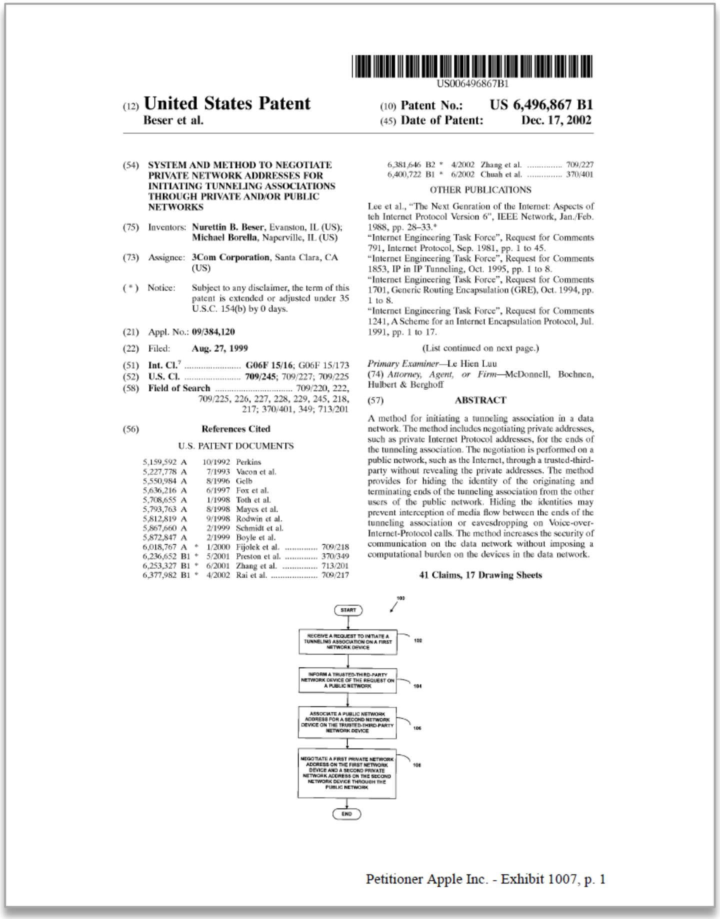
> In one exemplary preferred embodiment, the negotiation is carried out through the trusted-third-party network device,

Beser (Ex. 1007) at 9:29-30; Pet. (866) 21-22, 38

FIG. 6



Beser (Ex. 1007) at Fig. 6; Pet. (866) at 19-21



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**

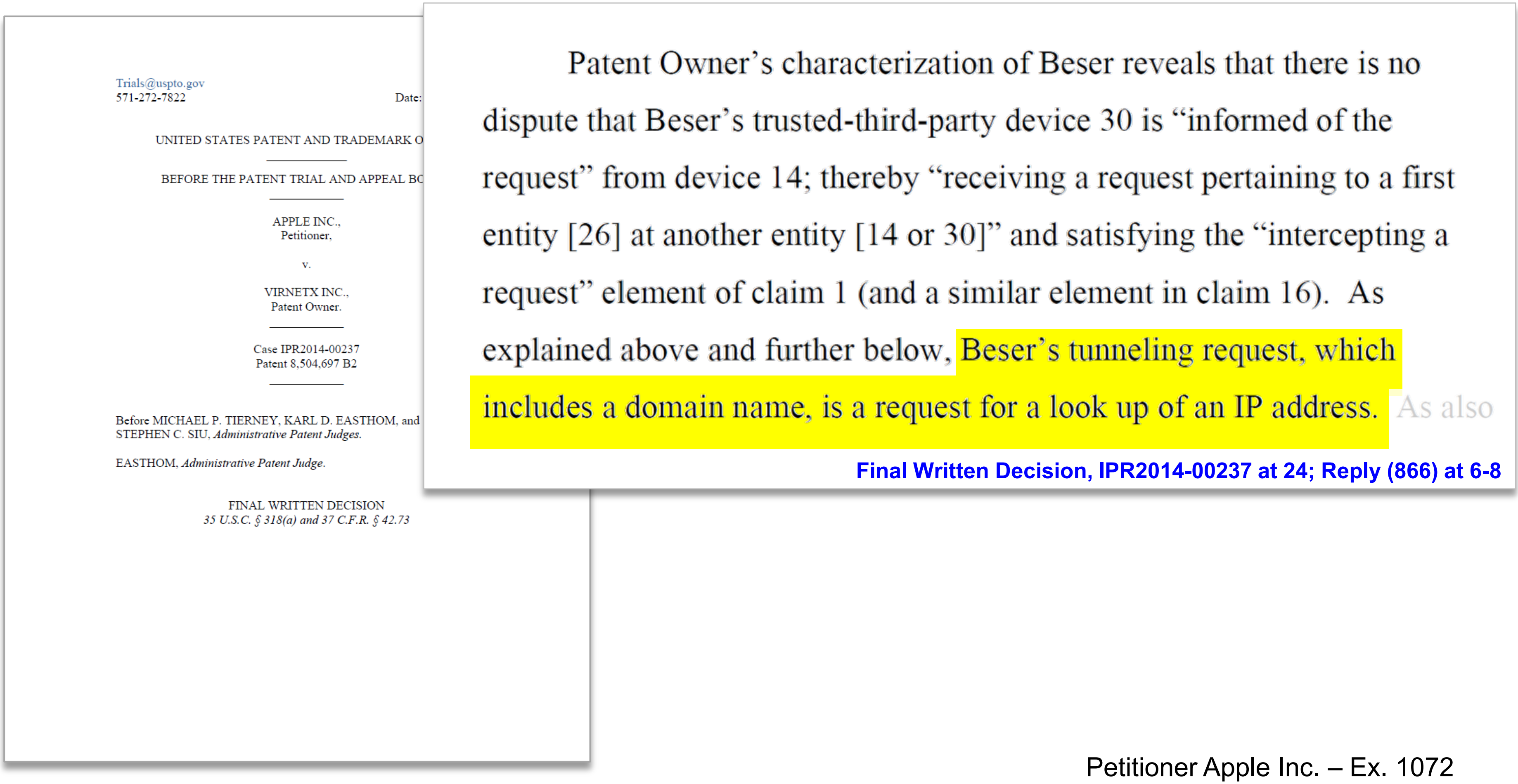
A method for initiating a tunneling association in a data network. The method includes negotiating private addresses, such as private Internet Protocol addresses, for the ends of the tunneling association. The negotiation is performed on a public network, such as the Internet, through a trusted-third-party 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

100
START
RECEIVE A REQUEST TO INITIATE A TUNNELING ASSOCIATION ON A FIRST NETWORK DEVICE
102
INFORM A TRUSTED-THIRD-PARTY NETWORK DEVICE OF THE REQUEST ON A PUBLIC NETWORK
104
ASSOCIATE A PUBLIC NETWORK ADDRESS FOR A SECOND NETWORK DEVICE ON THE TRUSTED-THIRD-PARTY NETWORK DEVICE
106
NEGOTIATE A FIRST PRIVATE NETWORK ADDRESS ON THE FIRST NETWORK DEVICE AND A SECOND PRIVATE NETWORK ADDRESS ON THE SECOND NETWORK DEVICE THROUGH THE PUBLIC NETWORK
108
END

Final Written Decision in IPR2014-00237

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



Trials@uspto.gov
571-272-7822

Date:

UNITED STATES PATENT AND TRADEMARK O

BEFORE THE PATENT TRIAL AND APPEAL BC

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2014-00237
Patent 8,504,697 B2

Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and
STEPHEN C. SIU, *Administrative Patent Judges.*

EASTHOM, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

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 (866) at 6-8

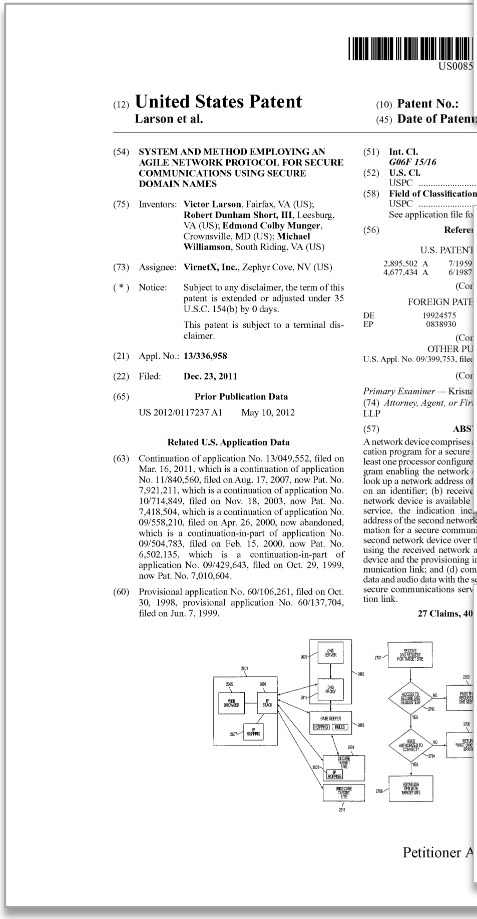
IPR2015-00866, -868, -870

Beser and RFC 2401 Issues

1. **Common Issues (866, 868, & 870)**
   - A. *"Virtual Private Network Communication Link" (866: claims; 868: claim 10; 870: claims 6 & 21)*
   - B. Encrypting audio/visual data
   - C. Combining Beser and RFC 2401 would have been obvious
   - D. A "*request to look up an []IP address… based on a domain name associated with the second network [target] device"*
   - **E. *"Interception of the request to look up an Internet Protocol (IP) address"***
2. **Issues Affecting 866 & 868 Only**
   - A. *"Receiv[ing]. . . An Indication [and] a Network Address"*
3. **Dependent Claims**
   - A. *"email" and "secure domain name"*

The Challenged Claims:

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



US0085

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

(10) **Patent No.:**
(45) **Date of Patent:** *Aug. 20, 2013

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,958**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0117237 A1 May 10, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file fo

(56) **Refere**

U.S. PATENT

2,895,502 A 7/1959
4,677,434 A 6/1987

(Cor

FOREIGN PATE

DE 19924575
EP 0838930

(Cor

OTHER PU

U.S. Appl. No. 09/399,753, filed

(Cor

Primary Examiner — Krisna
(74) *Attorney, Agent, or Fir* LLP

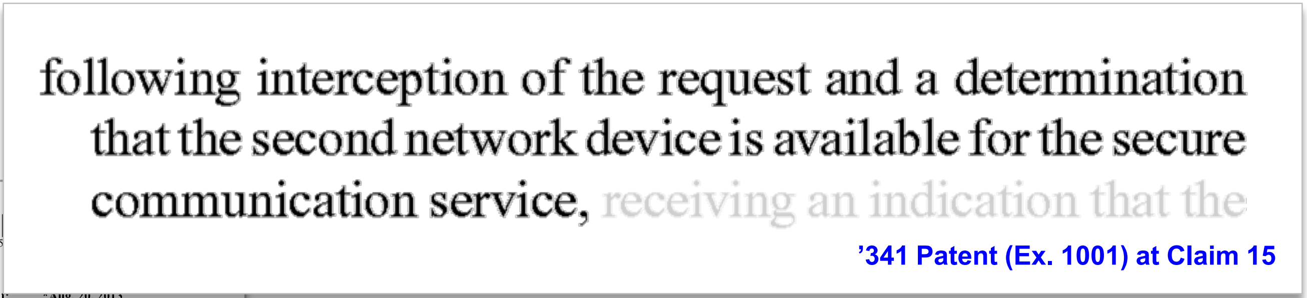
(57) **ABS**

A network device comprises a cation program for a secure least one processor configure gram enabling the network look up a network address of on an identifier; (b) receive network device is available service, the indication including the requested network address of the second network device and provisioning information for a secure communication link; (c) connect to the second network device over the secure communication link, using the received network address of the second network device and the provisioning information for the secure communication link; and (d) communicate at least one of video data and audio data with the second network device using the secure communications serv tion link.

27 Claims, 40

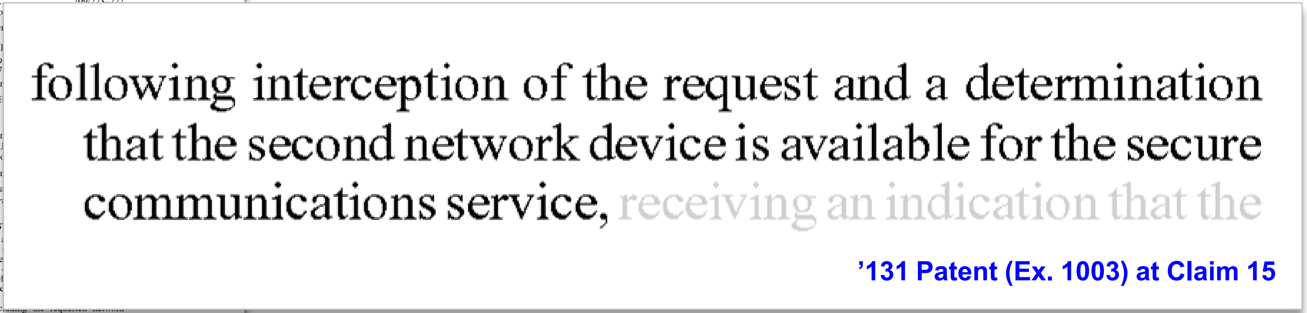
Petitioner A

2601
2605
2606
WEB BROWSER
IP STACK
2607
IP HOPPING
2609
DNS SERVER
2610
DNS PROXY
2602
GATE KEEPER
HOPPING RULES
2603
2604
SECURE TARGET SITE
IP HOPPING
UNSECURE TARGET SITE
2611
2701
RECEIVE DNS REQUEST FOR TARGET SITE
ACCESS TO SECURE SITE REQUESTED?
NO
2703
PASS TH REQUEST DNS SER
2702
YES
USER AUTHORIZED TO CONNECT?
NO
2705
RETUR "HOST UNK ERROR
2704
YES
ESTABLISH VPN WITH TARGET SITE
2706



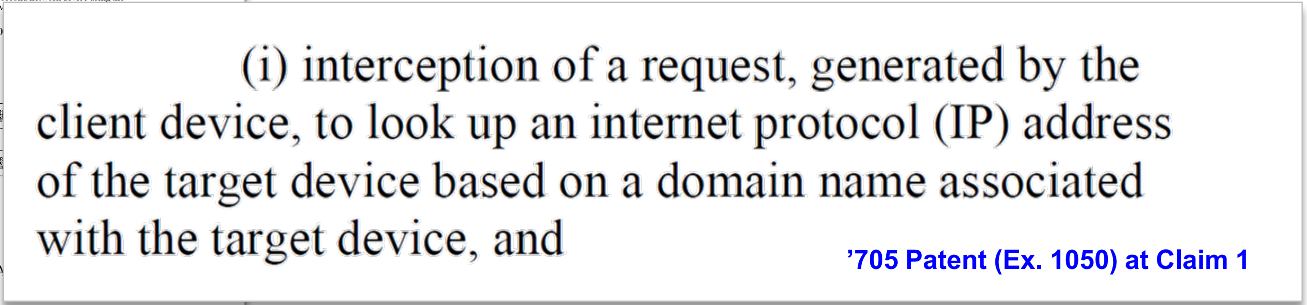
following interception of the request and a determination that the second network device is available for the secure communication service, receiving an indication that the

’341 Patent (Ex. 1001) at Claim 15



following interception of the request and a determination that the second network device is available for the secure communications service, receiving an indication that the

’131 Patent (Ex. 1003) at Claim 15

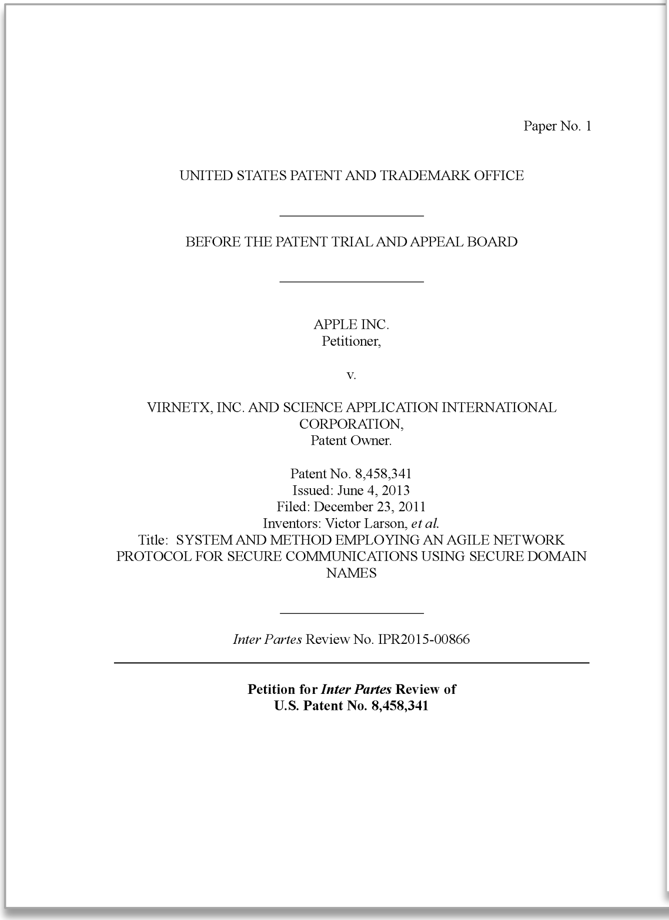


(i) interception of a request, generated by the client device, to look up an internet protocol (IP) address of the target device based on a domain name associated with the target device, and

’705 Patent (Ex. 1050) at Claim 1

Beser and RFC 2401

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



Paper No. 1

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

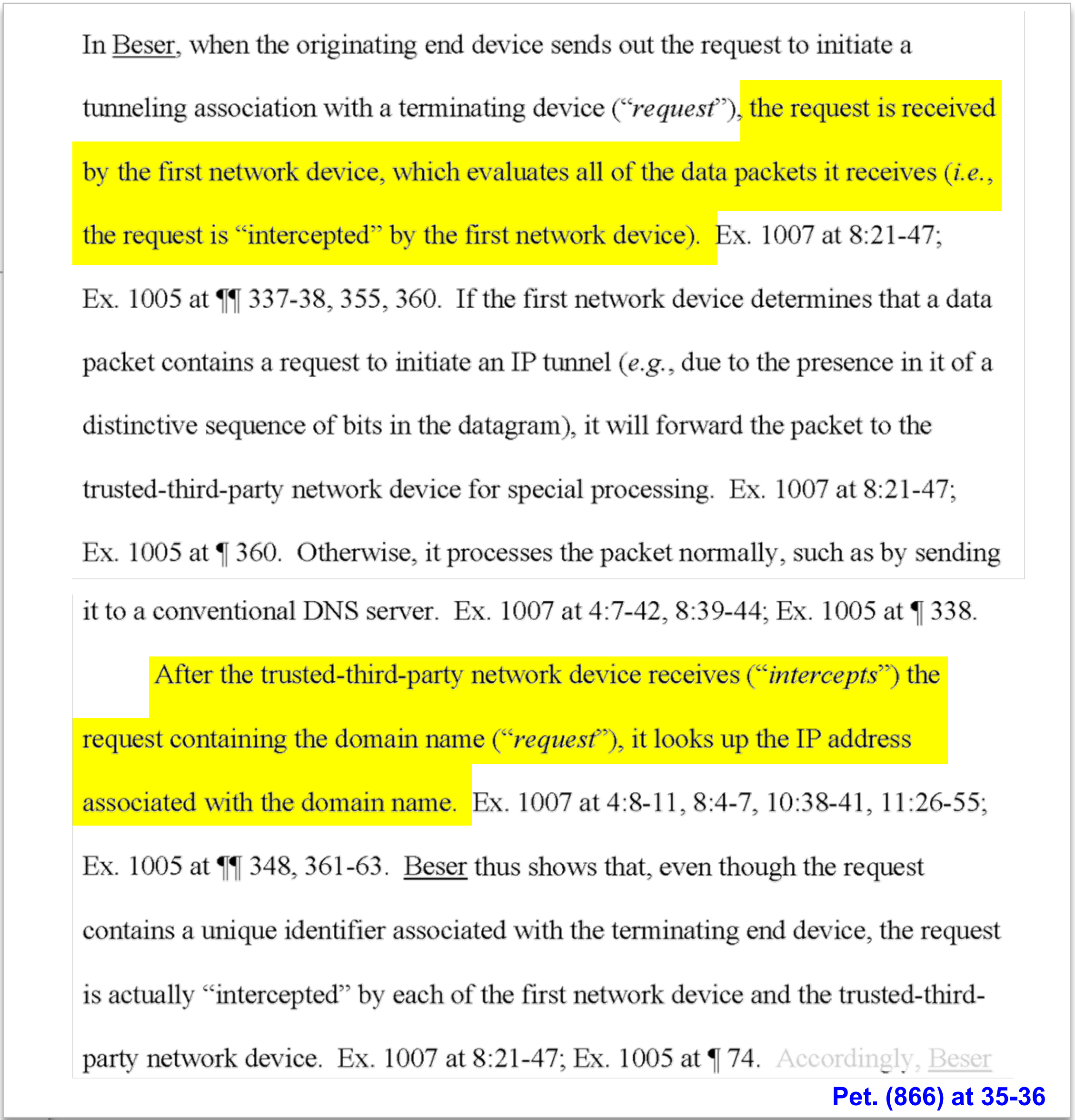
v.

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

Patent No. 8,458,341
Issued: June 4, 2013
Filed: December 23, 2011
Inventors: Victor Larson, *et al.*
Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Inter Partes Review No. IPR2015-00866

**Petition for *Inter Partes* Review of
U.S. Patent No. 8,458,341**



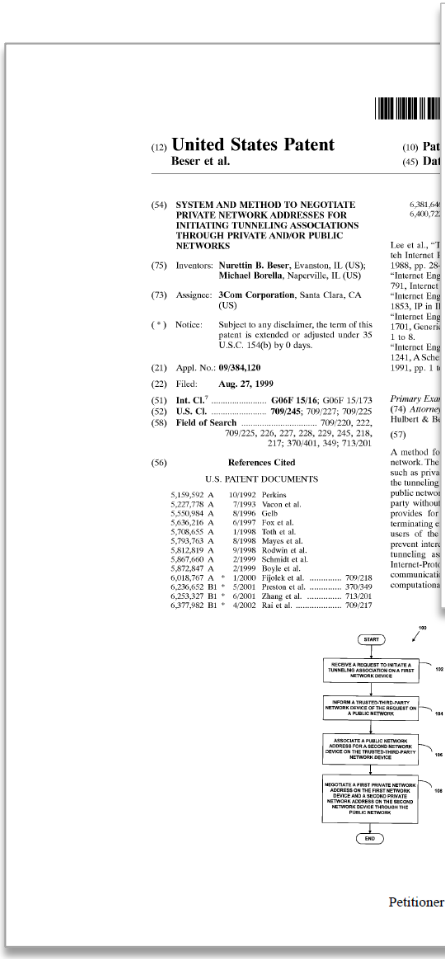
In Beser, when the originating end device sends out the request to initiate a tunneling association with a terminating device (“*request*”), the request is received by the first network device, which evaluates all of the data packets it receives (*i.e.*, the request is “intercepted” by the first network device). Ex. 1007 at 8:21-47; Ex. 1005 at ¶¶ 337-38, 355, 360. 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 ¶ 360. 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 ¶ 338.

After the trusted-third-party network device receives (“*intercepts*”) the request containing the domain name (“*request*”), it looks up the IP address associated with the domain name. Ex. 1007 at 4:8-11, 8:4-7, 10:38-41, 11:26-55; Ex. 1005 at ¶¶ 348, 361-63. Beser thus shows that, even though the request contains a unique identifier associated with the terminating end device, the request is actually “intercepted” by each of the first network device and the trusted-third-party network device. Ex. 1007 at 8:21-47; Ex. 1005 at ¶ 74. Accordingly, Beser

Pet. (866) at 35-36

Beser and RFC 2401

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



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

(10) **Pat**
(45) **Dat**

(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

6,381,64
6,400,72

Lee et al., “T
teh Internet I
1988, pp. 28-
“Internet Eng
791, Internet
“Internet Eng
1853, IP in II
“Internet Eng
1701, Generic
1 to 8.
“Internet Eng
1241, A Sche
1991, pp. 1 t

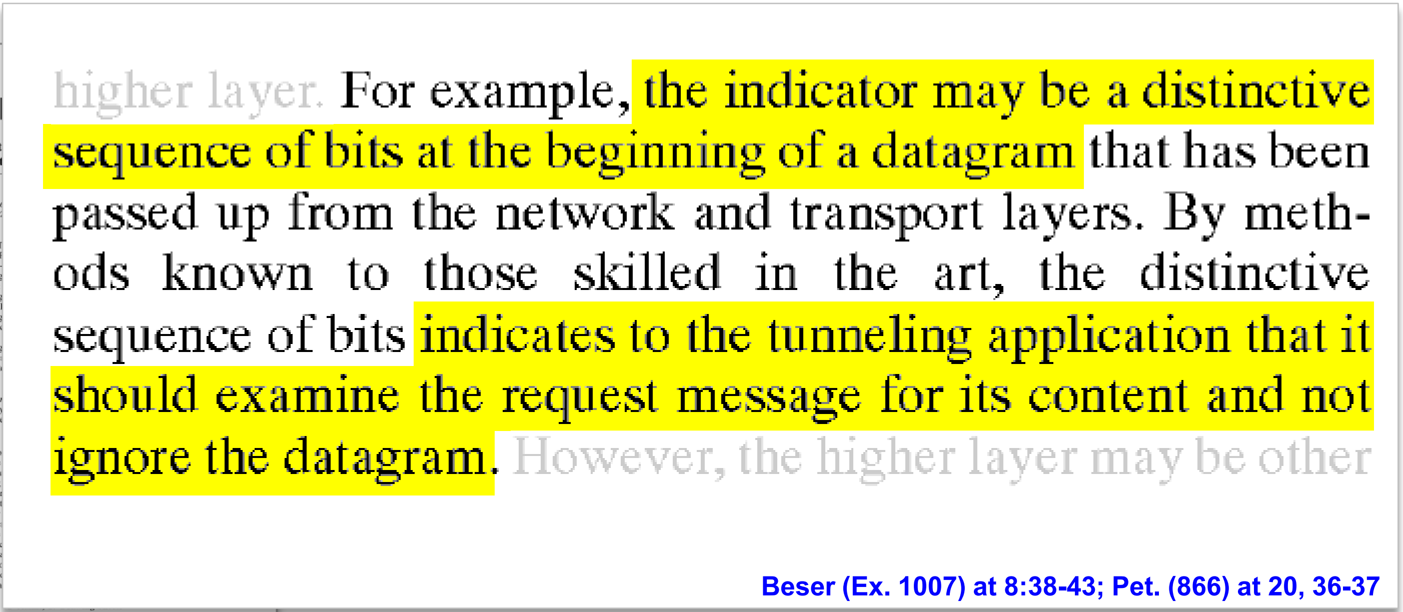
Primary Exa
(74) *Attorney*
Hulbert & B

(57)

A method fo
network. The
such as priva
the tunneling
public netwo
party without
provides for
terminating e
users of the
prevent interc
tunneling as
Internet-Prot
communicati
computationa

100
START
RECEIVE A REQUEST TO INITIATE A TUNNELING ASSOCIATION ON A FIRST NETWORK DEVICE
102
INFORM A TRUSTED-THIRD-PARTY NETWORK DEVICE OF THE REQUEST ON A PUBLIC NETWORK
104
ASSOCIATE A PUBLIC NETWORK ADDRESS FOR A SECOND NETWORK DEVICE ON THE TRUSTED-THIRD-PARTY NETWORK DEVICE
106
NEGOTIATE A FIRST PRIVATE NETWORK ADDRESS ON THE FIRST NETWORK DEVICE AND A SECOND PRIVATE NETWORK ADDRESS ON THE SECOND NETWORK DEVICE THROUGH THE PUBLIC NETWORK
108
END

Petitioner Apple Inc. - Exhibit 1007, p. 1

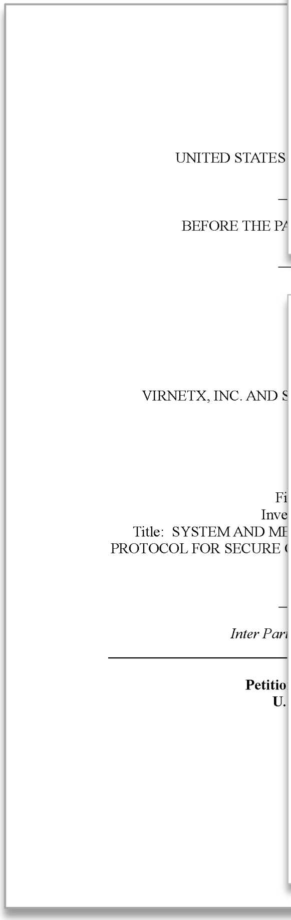


higher layer. For example, the indicator may be a distinctive sequence of bits at the beginning of a datagram that has been passed up from the network and transport layers. By methods known to those skilled in the art, the distinctive sequence of bits indicates to the tunneling application that it should 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. (866) at 20, 36-37

Beser and RFC 2401

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



UNITED STATES

BEFORE THE PA

VIRNETX, INC. AND S

Fi
Inve
Title: SYSTEM AND ME
PROTOCOL FOR SECURE C

Inter Part

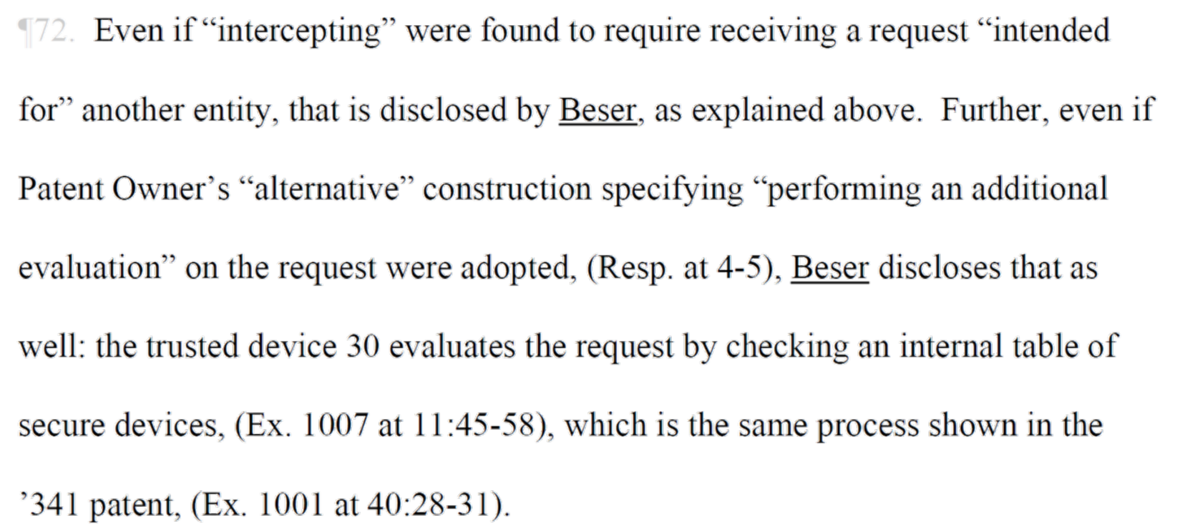
Petitio
U.

Interception of the Request

Petitioner's Construction	Patent Owner's Construction
Receiving a request pertaining to a first entity at another entity	No construction necessary; alternatively, receiving a request to look up an internet protocol address and, apart from resolving it into an address, performing an evaluation on it related to establishing a virtual private network communication link

Pet. (866) at 9-10; Resp. (866) at 8

Reply:

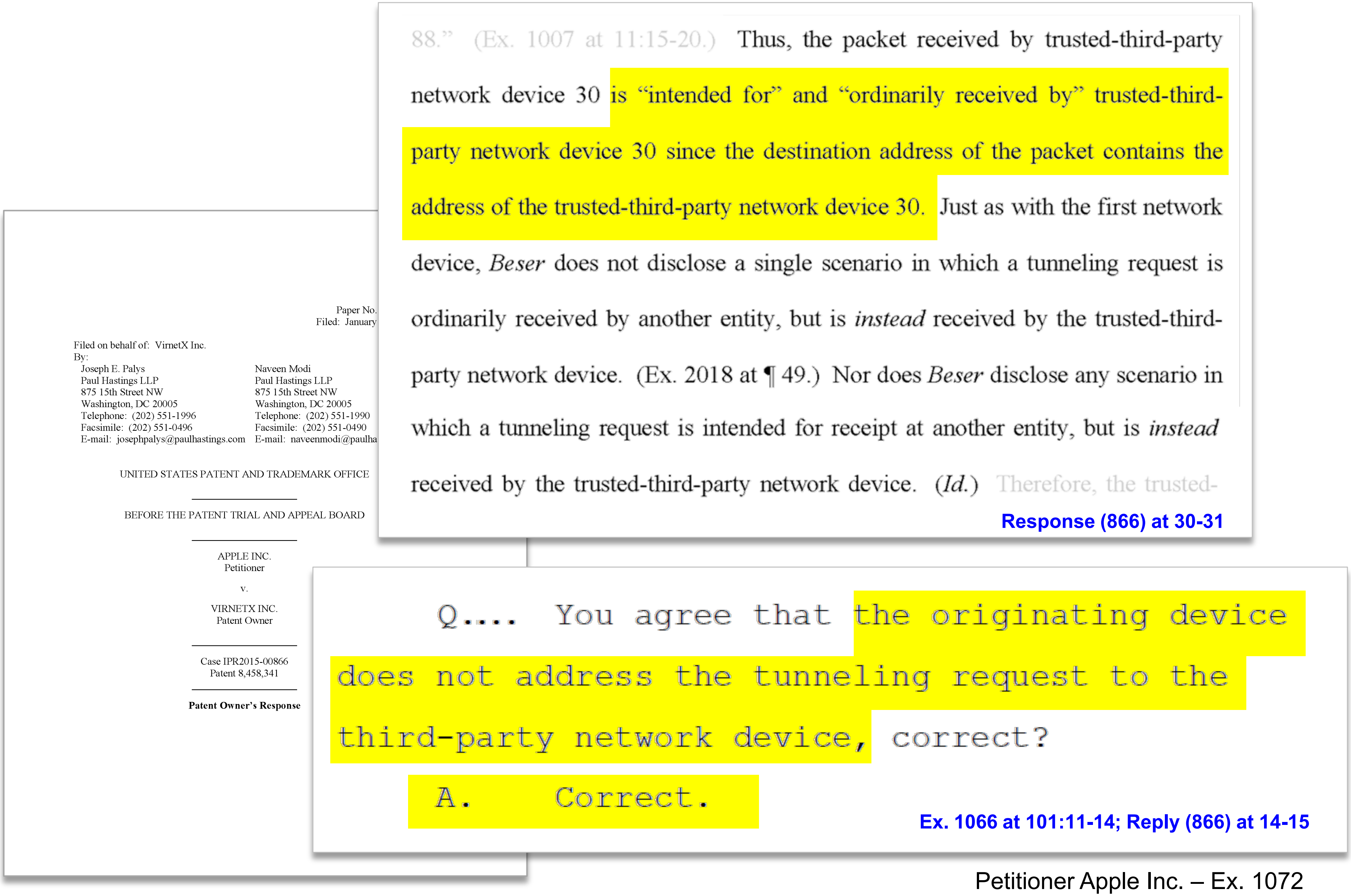


¶72. Even if "intercepting" were found to require receiving a request "intended for" another entity, that is disclosed by Beser, as explained above. Further, even if Patent Owner's "alternative" construction specifying "performing an additional evaluation" on the request were adopted, (Resp. at 4-5), Beser discloses that as well: the trusted device 30 evaluates the request by checking an internal table of secure devices, (Ex. 1007 at 11:45-58), which is the same process shown in the '341 patent, (Ex. 1001 at 40:28-31).

Reply (866) at 31

Patent Owner Admission

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



Paper No.
Filed: January

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 Modi
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-1990
Facsimile: (202) 551-0490
E-mail: naveenmodi@paulha

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2015-00866
Patent 8,458,341

Patent Owner's Response

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. 2018 at ¶ 49.) Nor does *Beser* disclose any scenario in which a tunneling request is intended for receipt at another entity, but is *instead* received by the trusted-third-party network device. (*Id.*) Therefore, the trusted-

Response (866) at 30-31

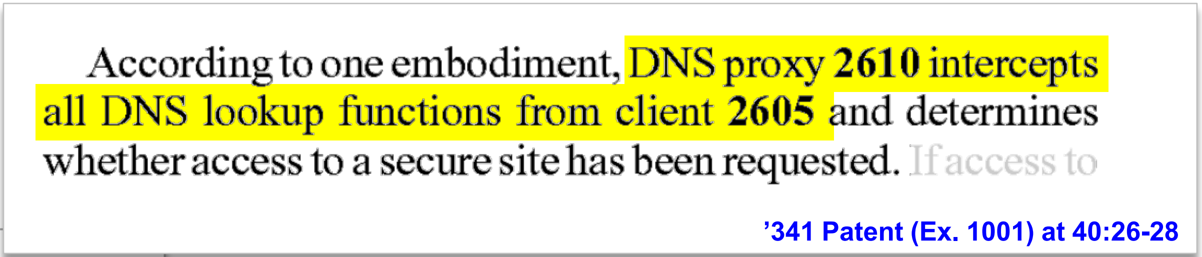
Q.... You agree that the originating device does not address the tunneling request to the third-party network device, correct?

A. Correct.

Ex. 1066 at 101:11-14; Reply (866) at 14-15

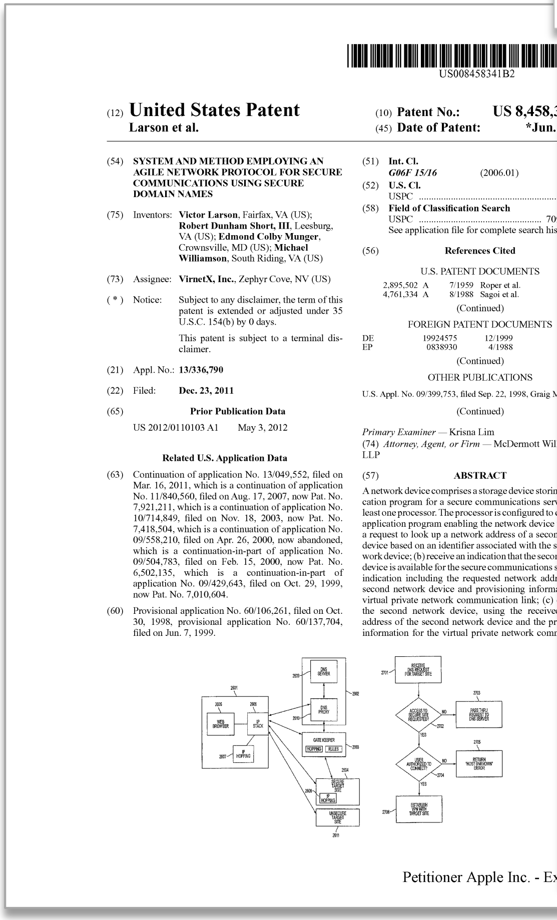
The Challenged Patents

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



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

'341 Patent (Ex. 1001) at 40:26-28



US008458341B2

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

(10) **Patent No.: US 8,458,3**
(45) **Date of Patent: *Jun.**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,790**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0110103 A1 May 3, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC ....

(58) **Field of Classification Search**
USPC 709
See application file for complete search hist

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,761,334	A	8/1988	Sagoi et al.

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

U.S. Appl. No. 09/399,753, filed Sep. 22, 1998, Graig Mi

(Continued)

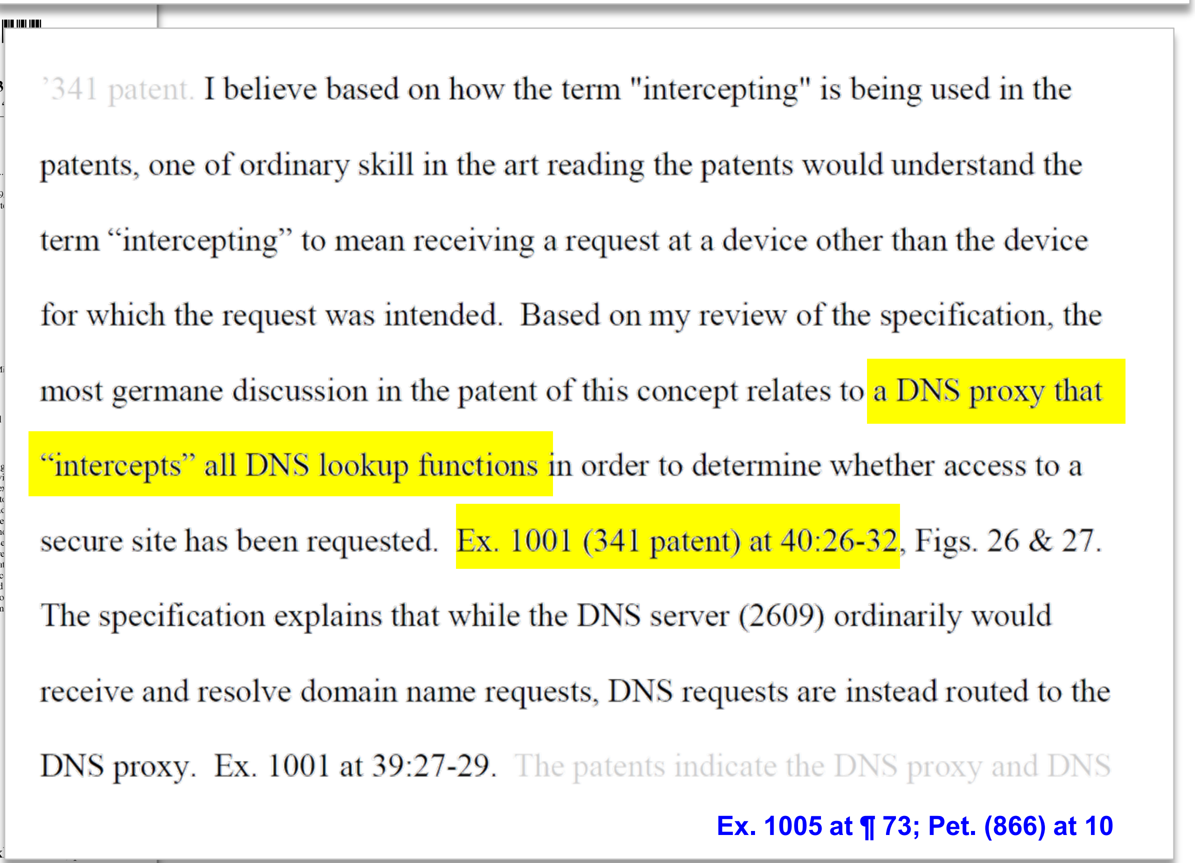
Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will
LLP

(57) **ABSTRACT**

A network device comprises a storage device storing cation program for a secure communications servi least one processor. The processor is configured to ex application program enabling the network device to a request to look up a network address of a second device based on an identifier associated with the se work device; (b) receive an indication that the second device is available for the secure communications se indication including the requested network addre second network device and provisioning informat virtual private network communication link; (c) c the second network device, using the received address of the second network device and the pro information for the virtual private network comm

DNS SERVER
2609
2601
2602
2605
2606
DNS PROXY
2610
RECEIVE DNS REQUEST FOR TARGET SITE
2701
ACCESS TO SECURE SITE REQUESTED?
NO
PASS THRU REQUEST TO DNS SERVER
2703

Petitioner Apple Inc. - Ex

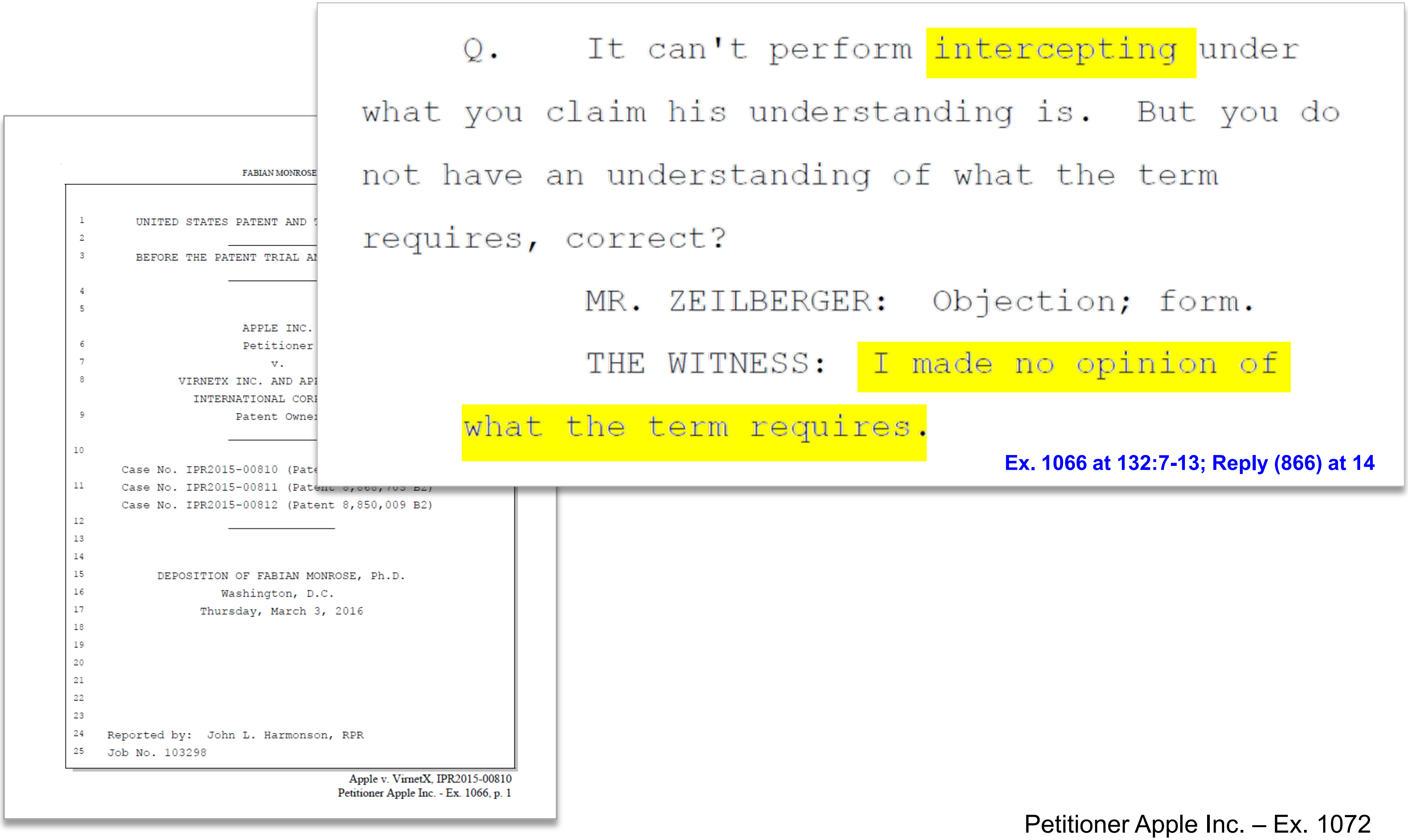


'341 patent. I believe based on how the term "intercepting" is being used in the patents, one of ordinary skill in the art reading the patents would understand the term "intercepting" to mean receiving a request at a device other than the device for which the request was intended. Based on my review 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 (341 patent) at 40:26-32, 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 at 39:27-29. The patents indicate the DNS proxy and DNS

Ex. 1005 at ¶ 73; Pet. (866) at 10

Patent Owner Admission

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



FABIAN MONROSE

UNITED STATES PATENT AND T

BEFORE THE PATENT TRIAL AN

APPLE INC.
Petitioner
v.
VIRNETX INC. AND API
INTERNATIONAL CORI
Patent Owner

Case No. IPR2015-00810 (Pate
Case No. IPR2015-00811 (Pate
Case No. IPR2015-00812 (Patent 8,850,009 B2)

DEPOSITION OF FABIAN MONROSE, Ph.D.
Washington, D.C.
Thursday, March 3, 2016

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?

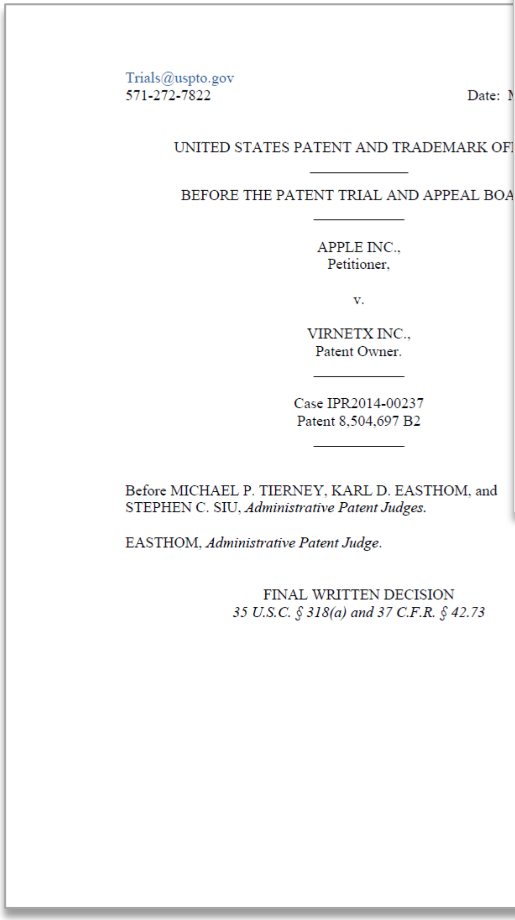
MR. ZEILBERGER: Objection; form.

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

Ex. 1066 at 132:7-13; Reply (866) 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

Date: M

UNITED STATES PATENT AND TRADEMARK OF

BEFORE THE PATENT TRIAL AND APPEAL BOA

APPLE INC.,
Petitioner,

v.

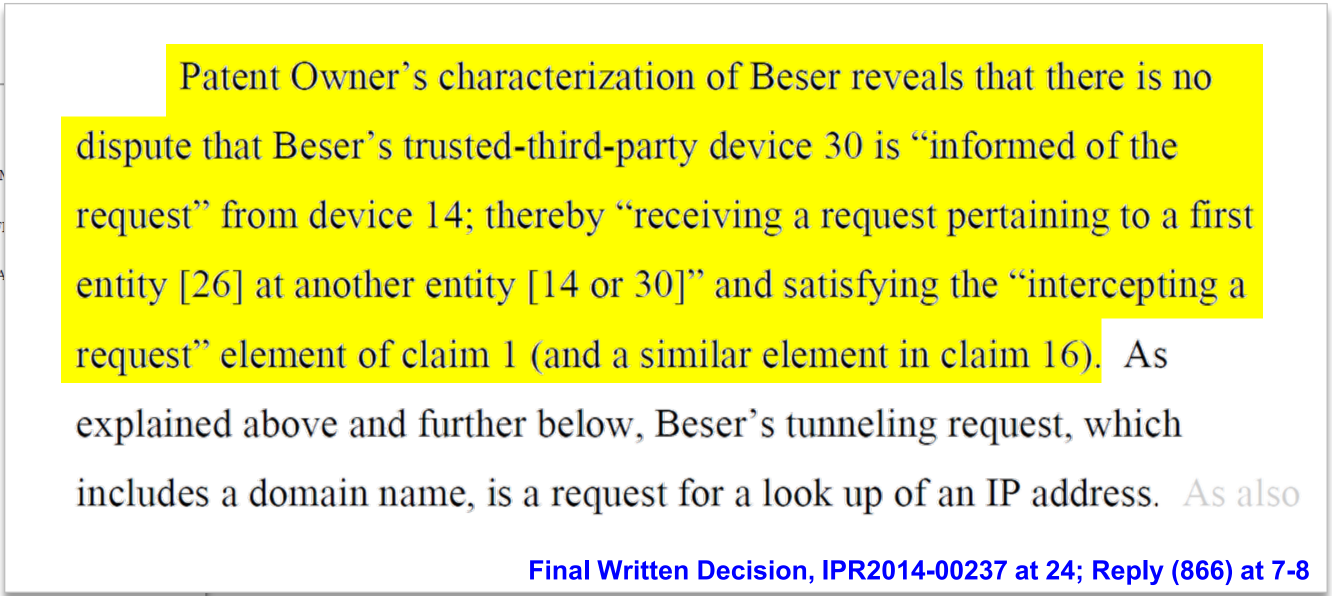
VIRNETX INC.,
Patent Owner.

Case IPR2014-00237
Patent 8,504,697 B2

Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and STEPHEN C. SIU, *Administrative Patent Judges.*

EASTHOM, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73



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 (866) at 7-8

IPR2015-00866, -868, -870

Beser and RFC 2401 Issues

1. **Common Issues (866, 868, & 870)**

   A. "Virtual Private Network Communication Link" (866: claims; 868: claim 10; 870: claims 6 & 21)

   B. Encrypting audio/visual data

   C. Combining Beser and RFC 2401 would have been obvious

   D. A "*request to look up an []IP address… based on a domain name associated with the second network [target] device*"

   E. "*Interception of the request to look up an Internet Protocol (IP) address*"

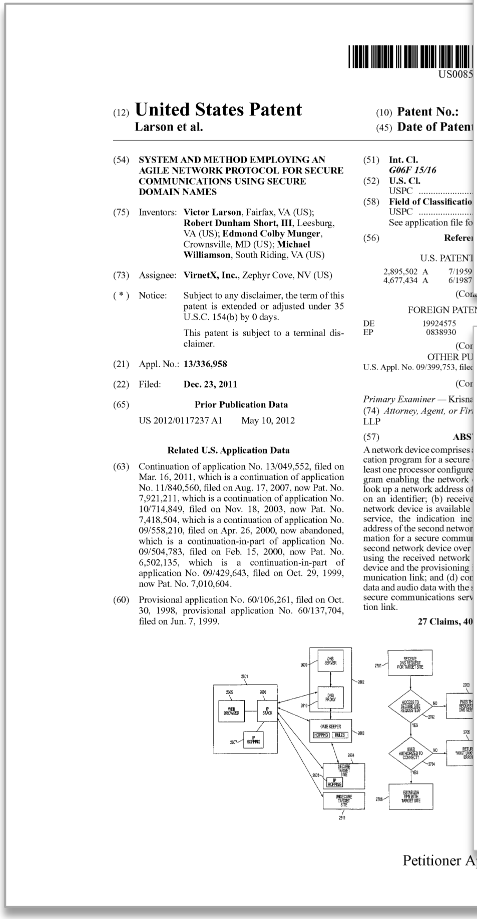
2. **Issues Affecting 866 & 868 Only**

   A. "Receiv[ing]. . . An Indication [and] a Network Address"

3. **Dependent Claims**

   A. "email" and "secure domain name"

The ’341 and ’131 Claims:
“*receiving*” an “*indication*” and the “*requested IP address*”



US0085

(12) United States Patent
Larson et al.

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

(54) SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,958**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0117237 A1 May 10, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16
(52) **U.S. Cl.**
USPC ....
(58) **Field of Classificatio**
USPC ....
See application file fo

(56) **Referer**

U.S. PATENT

2,895,502 A 7/1959
4,677,434 A 6/1987

(Continued)

FOREIGN PATENT DOCUMENTS

DE 19924575 12/1999
EP 0838930

(Cor

OTHER PU

U.S. Appl. No. 09/399,753, filec

(Cor

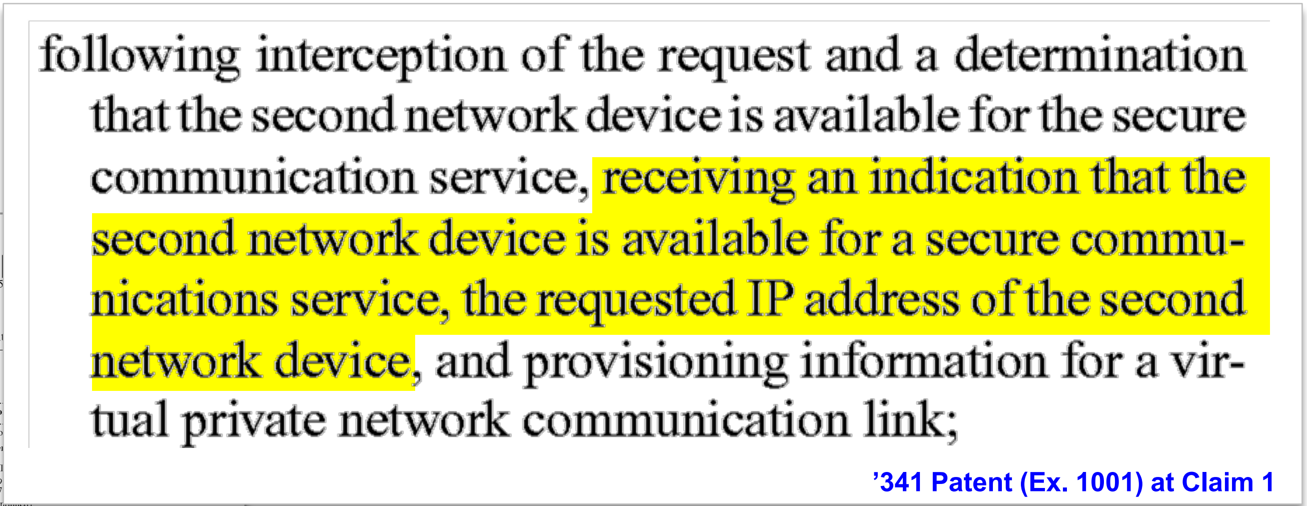
Primary Examiner — Krisna
(74) *Attorney, Agent, or Fir*
LLP

(57) **ABS**

A network device comprises
cation program for a secure
least one processor configure
gram enabling the network
look up a network address of
on an identifier; (b) receive
network device is available
service, the indication inc
address of the second networ
mation for a secure commu
second network device over
using the received network
device and the provisioning
munication link; and (d) cor
data and audio data with the
secure communications serv
tion link.

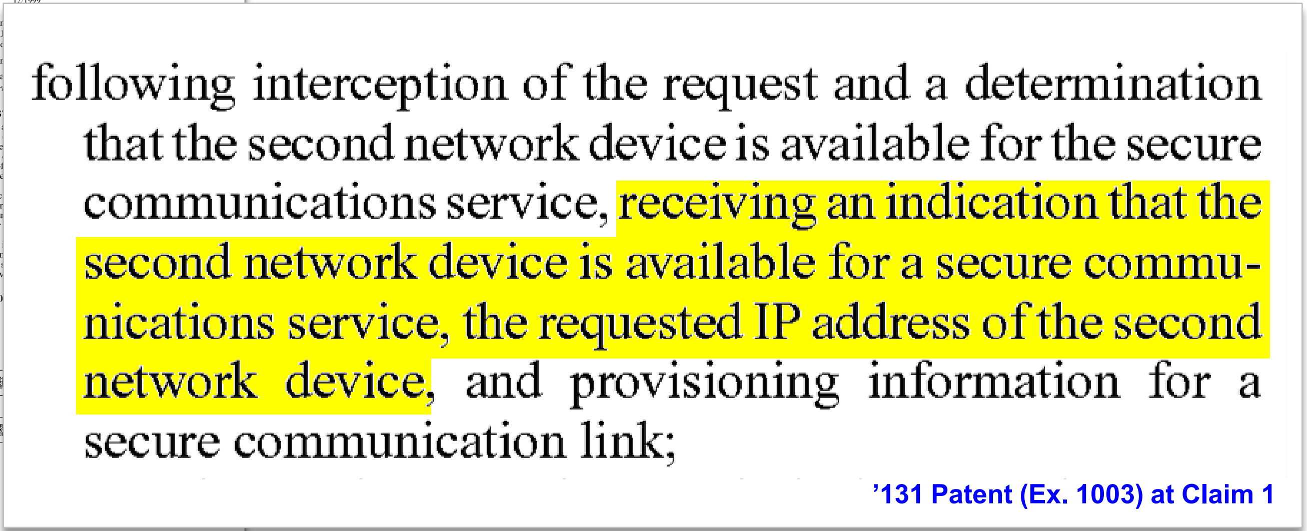
27 Claims, 40

Petitioner Apple Inc. - Exhibit 1003, p. 1



following interception of the request and a determination that the second network device is available for the secure communication service, receiving an indication that the second network device is available for a secure communications service, the requested IP address of the second network device, and provisioning information for a virtual private network communication link;

’341 Patent (Ex. 1001) at Claim 1



following interception of the request and a determination that the second network device is available for the secure communications service, receiving an indication that the second network device is available for a secure communications service, the requested IP address of the second network device, and provisioning information for a secure communication link;

’131 Patent (Ex. 1003) at Claim 1

Patent Owner Assertion

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

Case No. I

Pape
Filed: Dece

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 Modi
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-1
Facsimile: (202) 551-04
E-mail: naveenmodi@p

UNITED STATES PATENT AND TRADEMARK OFFI

BEFORE THE PATENT TRIAL AND APPEAL BOAR

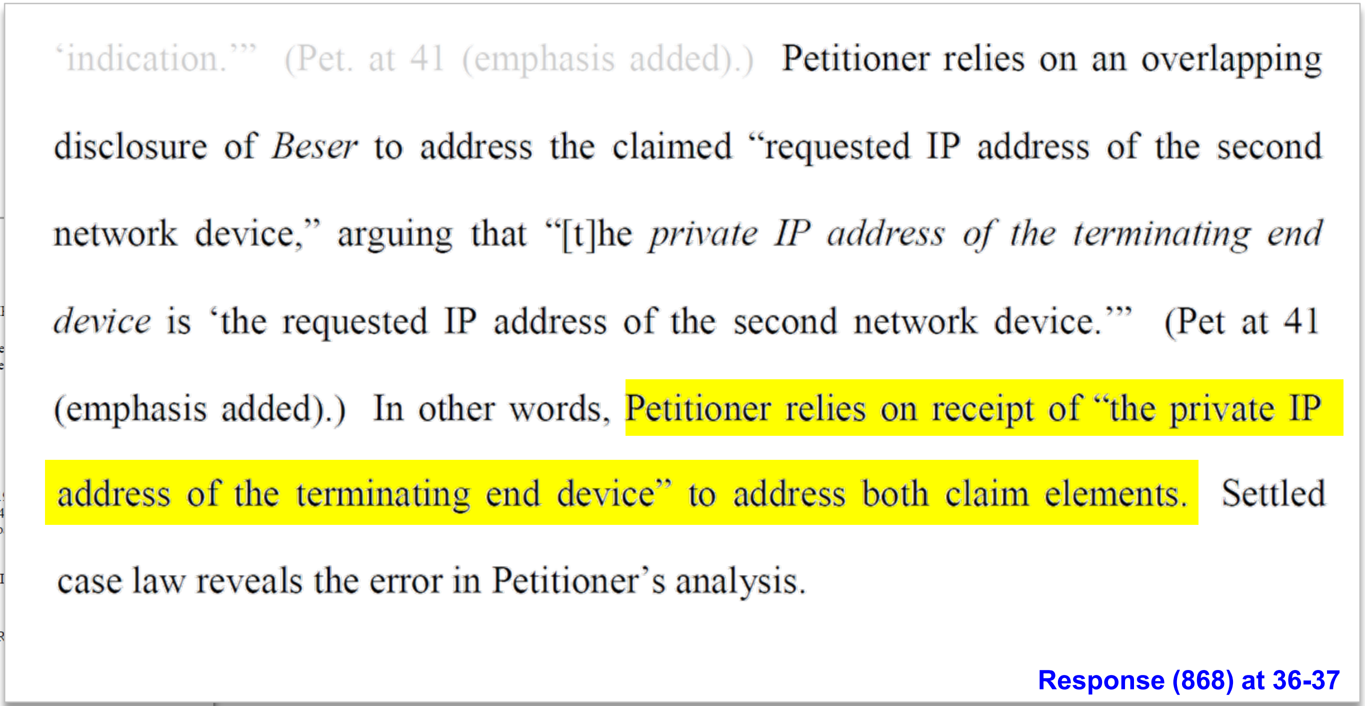
APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2015-00810
Patent 8,868,705

Patent Owner's Response

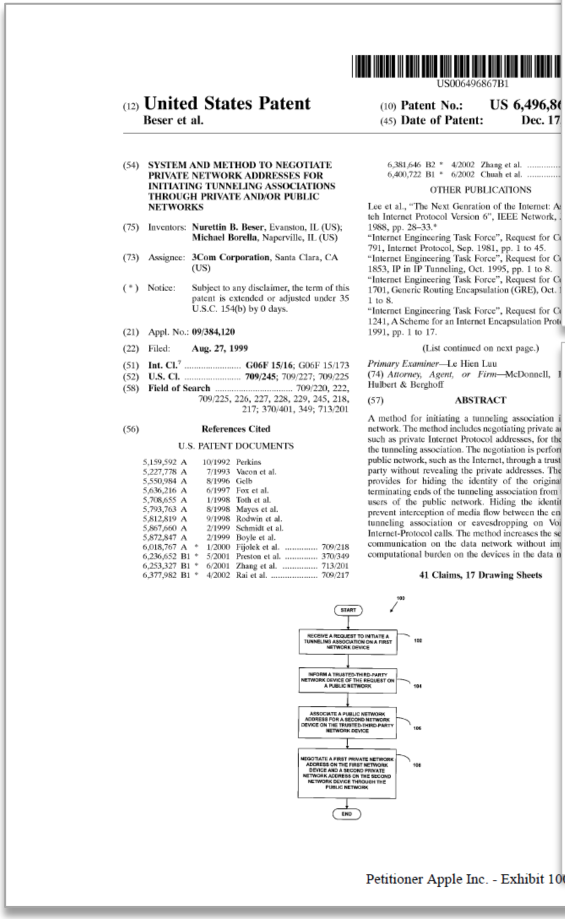


'indication.'" (Pet. at 41 (emphasis added).) Petitioner relies on an overlapping disclosure of *Beser* to address the claimed "requested IP address of the second network device," arguing that "[t]he *private IP address of the terminating end device* is 'the requested IP address of the second network device.'" (Pet at 41 (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 (868) at 36-37

Grounds Based on Beser and RFC 2401

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



US006496867B1

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

(10) **Patent No.:** **US 6,496,86**
(45) **Date of Patent:** **Dec. 17,**

(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.	
6,400,722	B1	*	6/2002	Chuah et al.	

OTHER PUBLICATIONS

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

(List continued on next page.)

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

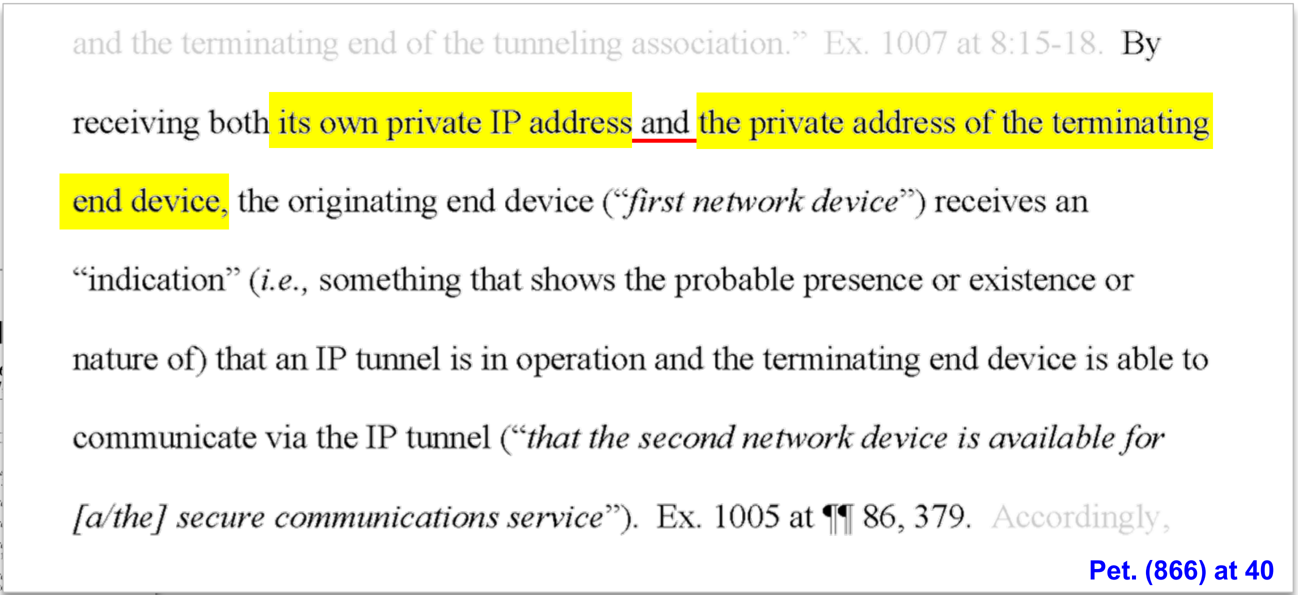
(57) **ABSTRACT**

A method for initiating a tunneling association i network. The method includes negotiating private a such as private Internet Protocol addresses, for the the tunneling association. The negotiation is perfor public network, such as the Internet, through a trust party without revealing the private addresses. The provides for hiding the identity of the originat terminating ends of the tunneling association from users of the public network. Hiding the identit prevent interception of media flow between the en tunneling association or eavesdropping on Voi Internet-Protocol calls. The method increases the se communication on the data network without im computational burden on the devices in the data n

41 Claims, 17 Drawing Sheets

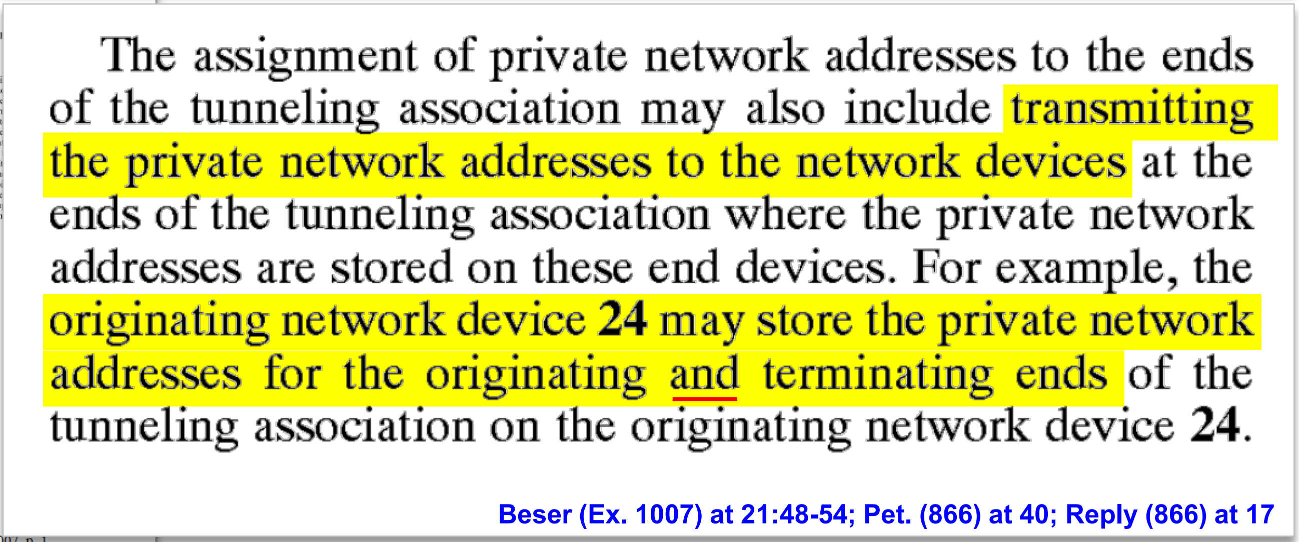
100
START
RECEIVE A REQUEST TO INITIATE A TUNNELING ASSOCIATION ON A FIRST NETWORK DEVICE
102
INFORM A TRUSTED-THIRD-PARTY NETWORK DEVICE OF THE REQUEST ON A PUBLIC NETWORK
104
ASSOCIATE A PUBLIC NETWORK ADDRESS FOR A SECOND NETWORK DEVICE ON THE TRUSTED-THIRD-PARTY NETWORK DEVICE
106
NEGOTIATE A FIRST PRIVATE NETWORK ADDRESS ON THE FIRST NETWORK DEVICE AND A SECOND PRIVATE NETWORK ADDRESS ON THE SECOND NETWORK DEVICE THROUGH THE PUBLIC NETWORK
108
END

Petitioner Apple Inc. - Exhibit 1007, p. 1



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 [a/the] secure communications service*"). Ex. 1005 at ¶¶ 86, 379. Accordingly,

Pet. (866) at 40



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. (866) at 40; Reply (866) at 17

IPR2015-00866, -868, -870

Beser and RFC 2401 Issues

1. **Common Issues (866, 868, & 870)**

   A. *"Virtual Private Network Communication Link" (866: claims; 868: claim 10; 870: claims 6 & 21)*

   B. Encrypting audio/visual data

   C. Combining Beser and RFC 2401 would have been obvious

   D. A "*request to look up an []IP address… based on a domain name associated with the second network [target] device"*

   E. "*Interception of the request to look up an Internet Protocol (IP) address"*

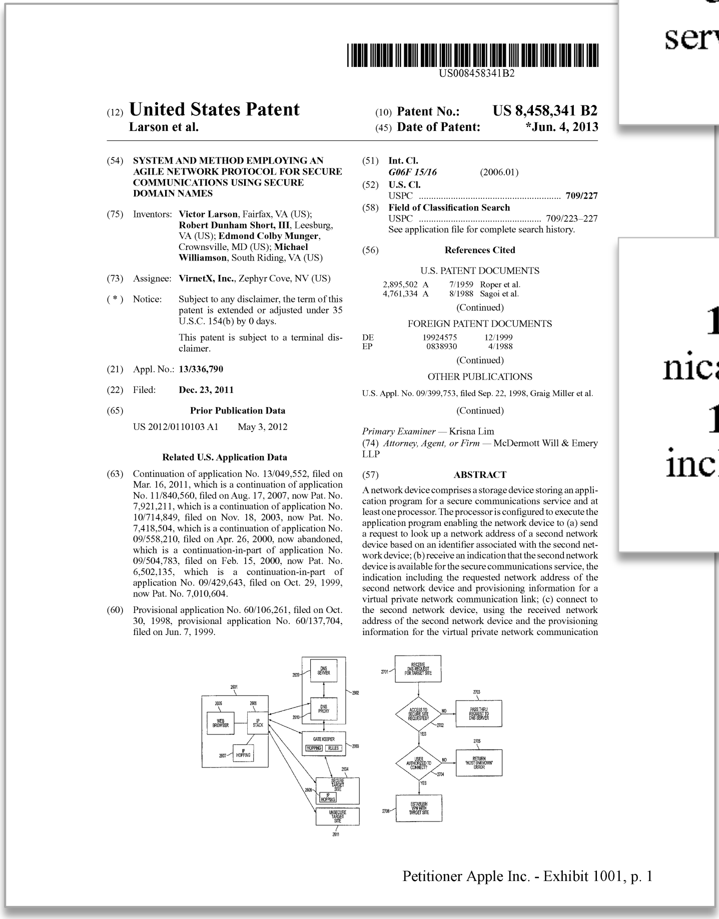
2. **Issues Affecting 866 & 868 Only**

   A. *"Receiv[ing]. . . An Indication [and] a Network Address"*

3. **Dependent Claims**

   A. "email" and "secure domain name"

’341 Patent, Claim 4, 5, 18, and 19



US008458341B2

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

(10) **Patent No.:** **US 8,458,341 B2**
(45) **Date of Patent:** ***Jun. 4, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,790**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0110103 A1 May 3, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,761,334	A	8/1988	Sagoi et al.

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

U.S. Appl. No. 09/399,753, filed Sep. 22, 1998, Graig Miller et al.

(Continued)

Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

A network device comprises a storage device storing an application program for a secure communications service and at least one processor. The processor is configured to execute the application program enabling the network device to (a) send a request to look up a network address of a second network device based on an identifier associated with the second network device; (b) receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link; (c) connect to the second network device, using the received network address of the second network device and the provisioning information for the virtual private network communication

Petitioner Apple Inc. - Exhibit 1001, p. 1

4. The network device of claim **1**, wherein the secure communications service includes a messaging service.

5. The network device of claim **4**, wherein the messaging service includes an e-mail service.

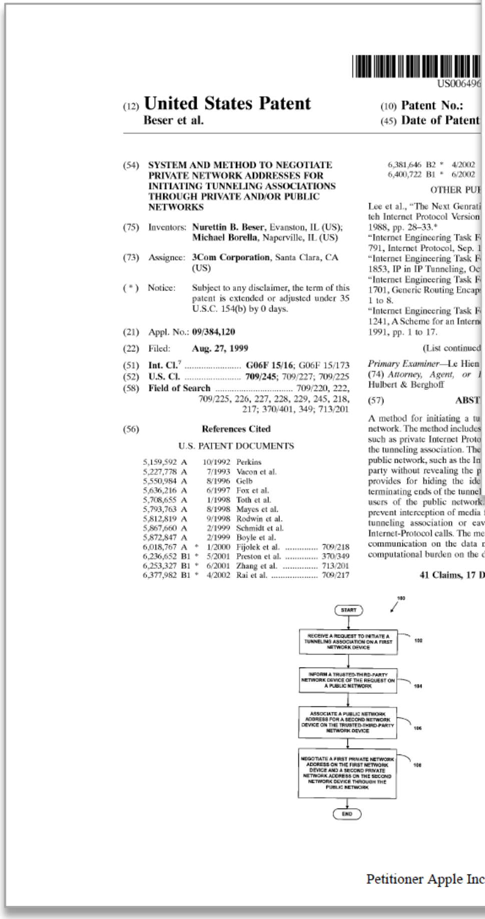
18. The method of claim **15**, wherein the secure communications service includes a messaging service.

19. The method of claim **18**, wherein the messaging service includes an e-mail service.

’341 Patent (Ex. 1001) at Claim 4, 5, 18, and 19

Beser and RFC 2401

“email”



US006496

(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
6,381,646	B2	*	4/2002		
6,400,722	B1	*	6/2002		

OTHER PUI

Lee et al., “The Next Genrati teh Internet Protocol Version 1988, pp. 28–33.*
“Internet Engineering Task F 791, Internet Protocol, Sep. 1
“Internet Engineering Task F 1853, IP in IP Tunneling, Oc
“Internet Engineering Task F 1701, Generic Routing Encap 1 to 8.
“Internet Engineering Task F 1241, A Scheme for an Intern 1991, pp. 1 to 17.

(List continued

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

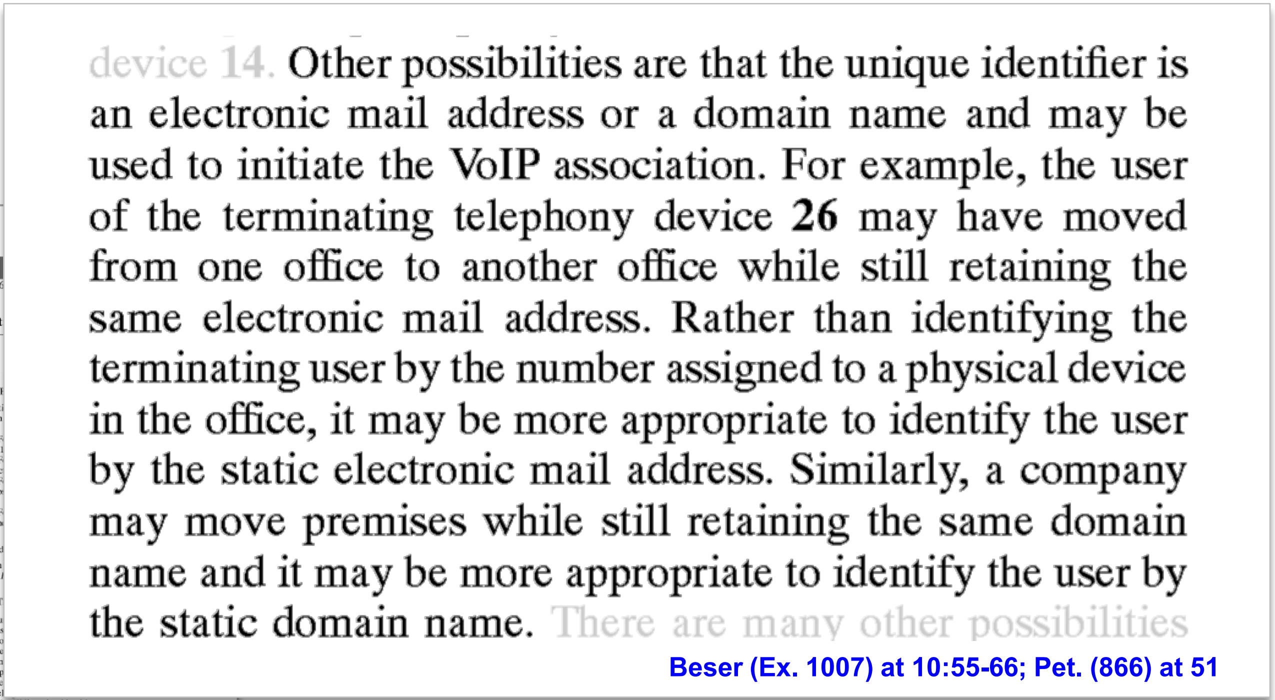
(57) ABST

A method for initiating a tu network. The method includes such as private Internet Proto the tunneling association. The public network, such as the In party without revealing the p provides for hiding the ide terminating ends of the tunnel 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

100
START
RECEIVE A REQUEST TO INITIATE A TUNNELING ASSOCIATION ON A FIRST NETWORK DEVICE
102
INFORM A TRUSTED-THIRD-PARTY NETWORK DEVICE OF THE REQUEST ON A PUBLIC NETWORK
104
ASSOCIATE A PUBLIC NETWORK ADDRESS FOR A SECOND NETWORK DEVICE ON THE TRUSTED-THIRD-PARTY NETWORK DEVICE
106
NEGOTIATE A FIRST PRIVATE NETWORK ADDRESS ON THE FIRST NETWORK DEVICE AND A SECOND PRIVATE NETWORK ADDRESS ON THE SECOND NETWORK DEVICE THROUGH THE PUBLIC NETWORK
108
END

Petitioner Apple Inc. - Exhibit 1007, p. 1

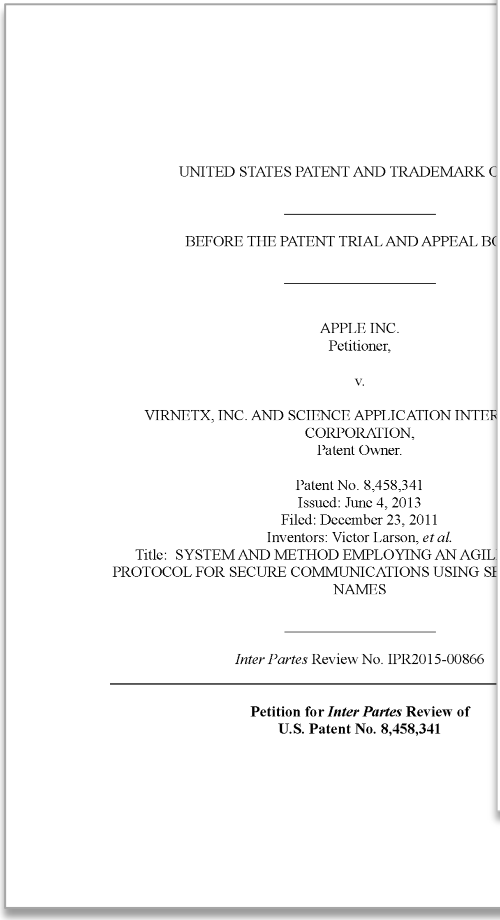


device 14. Other possibilities are that the unique identifier is an electronic mail address or a domain name and may be used to initiate the VoIP association. For example, the user of the terminating telephony device **26** may have moved from one office to another office while still retaining the same electronic mail address. Rather than identifying the terminating user by the number assigned to a physical device in the office, it may be more appropriate to identify the user by the static electronic mail address. Similarly, a company may move premises while still retaining the same domain name and it may be more appropriate to identify the user by the static domain name. There are many other possibilities

Beser (Ex. 1007) at 10:55-66; Pet. (866) at 51

Beser and RFC 2401

"email"



UNITED STATES PATENT AND TRADEMARK O

BEFORE THE PATENT TRIAL AND APPEAL BO

APPLE INC.
Petitioner,

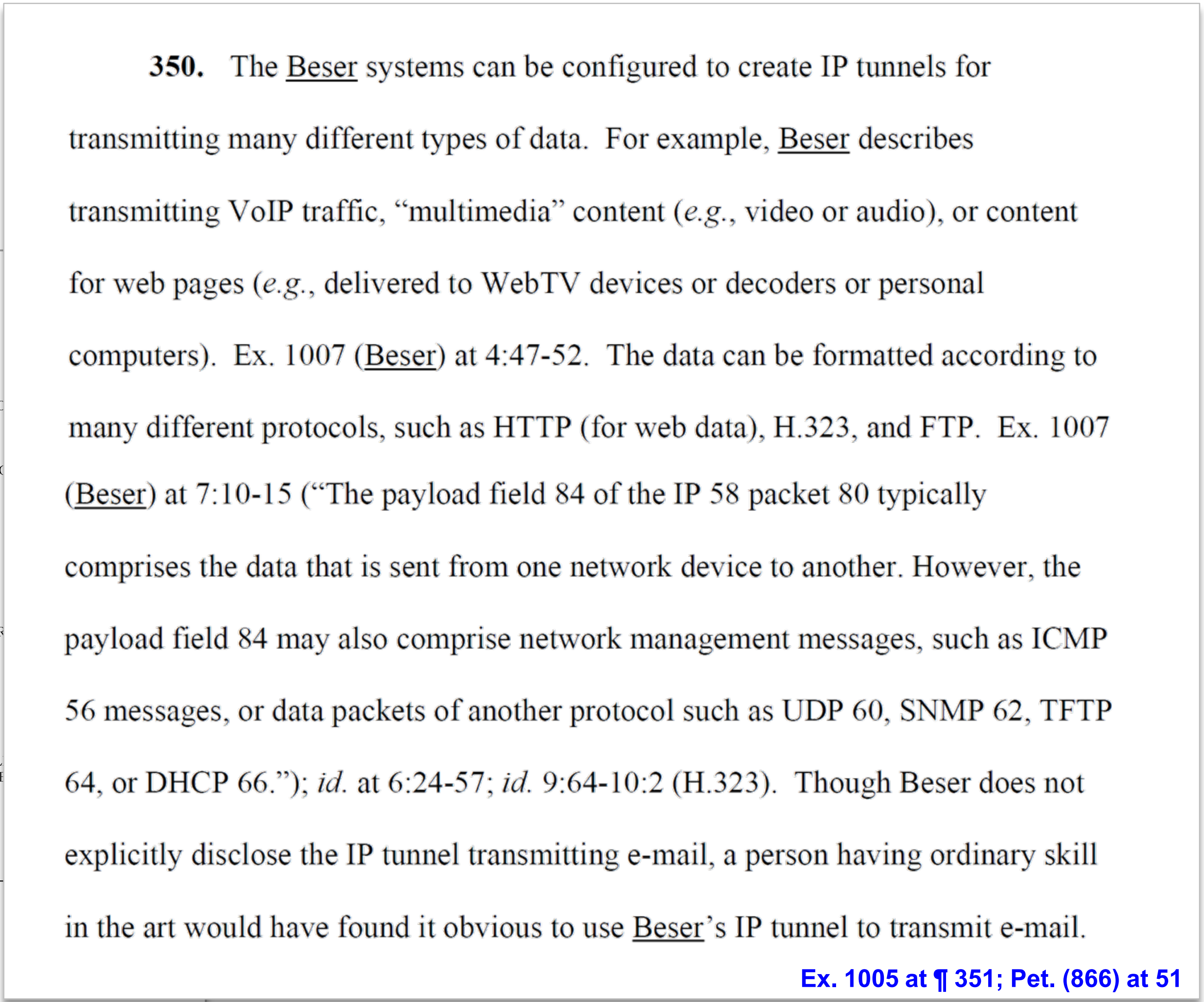
v.

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

Patent No. 8,458,341
Issued: June 4, 2013
Filed: December 23, 2011
Inventors: Victor Larson, *et al.*
Title: SYSTEM AND METHOD EMPLOYING AN AGIL
PROTOCOL FOR SECURE COMMUNICATIONS USING SE
NAMES

Inter Partes Review No. IPR2015-00866

Petition for *Inter Partes* Review of
U.S. Patent No. 8,458,341



350. The Beser systems can be configured to create IP tunnels for transmitting many different types of data. For example, Beser describes transmitting VoIP traffic, "multimedia" content (*e.g.*, video or audio), or content for web pages (*e.g.*, delivered to WebTV devices or decoders or personal computers). Ex. 1007 (Beser) at 4:47-52. The data can be formatted according to many different protocols, such as HTTP (for web data), H.323, and FTP. Ex. 1007 (Beser) at 7:10-15 ("The payload field 84 of the IP 58 packet 80 typically comprises the data that is sent from one network device to another. However, the payload field 84 may also comprise network management messages, such as ICMP 56 messages, or data packets of another protocol such as UDP 60, SNMP 62, TFTP 64, or DHCP 66."); *id.* at 6:24-57; *id.* 9:64-10:2 (H.323). Though Beser does not explicitly disclose the IP tunnel transmitting e-mail, a person having ordinary skill in the art would have found it obvious to use Beser's IP tunnel to transmit e-mail.

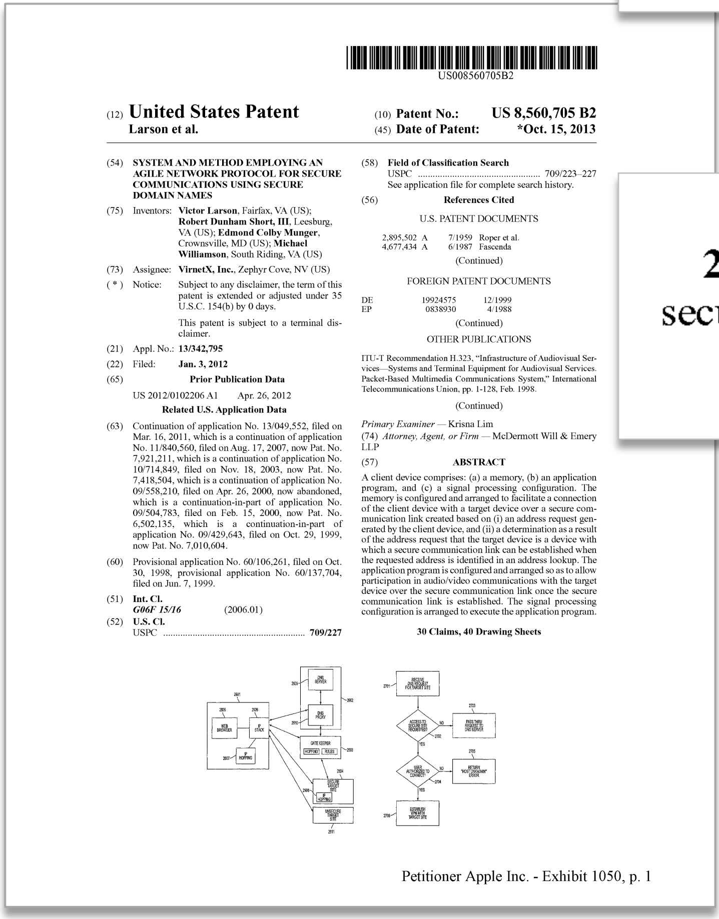
Ex. 1005 at ¶ 351; Pet. (866) at 51

’705 Patent, Claim 7 and 22

7. The client device of claim 3, wherein the domain name is a secure domain name.

22. The method of claim 16, wherein the domain name is a secure domain name.

’705 Patent (Ex. 1050) at Claim 7 and 22



US008560705B2

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

(10) **Patent No.:** **US 8,560,705 B2**
(45) **Date of Patent:** ***Oct. 15, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/342,795**

(22) Filed: **Jan. 3, 2012**

(65) **Prior Publication Data**

US 2012/0102206 A1 Apr. 26, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,677,434	A	6/1987	Fascenda

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

ITU-T Recommendation H.323, “Infrastructure of Audiovisual Services—Systems and Terminal Equipment for Audiovisual Services. Packet-Based Multimedia Communications System,” International Telecommunications Union, pp. 1-128, Feb. 1998.

(Continued)

Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

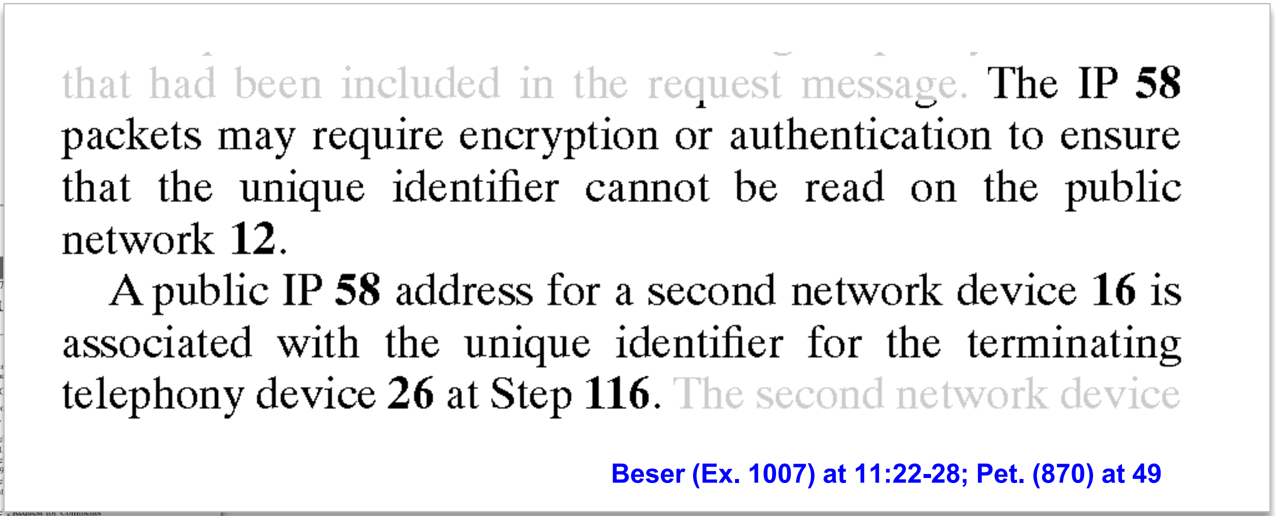
A client device comprises: (a) a memory, (b) an application program, and (c) a signal processing configuration. The memory is configured and arranged to facilitate a connection of the client device with a target device over a secure communication link created based on (i) an address request generated by the client device, and (ii) a determination as a result of the address request that the target device is a device with which a secure communication link can be established when the requested address is identified in an address lookup. The application program is configured and arranged so as to allow participation in audio/video communications with the target device over the secure communication link once the secure communication link is established. The signal processing configuration is arranged to execute the application program.

30 Claims, 40 Drawing Sheets

Petitioner Apple Inc. - Exhibit 1050, p. 1

Beser and RFC 2401

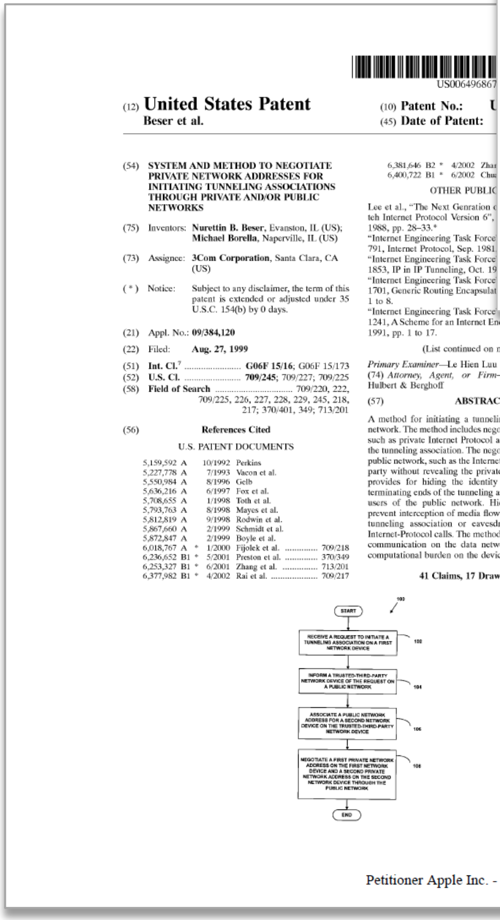
“secure domain name”



that had been included in the request message. The IP **58** packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network **12**.

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

Beser (Ex. 1007) at 11:22-28; Pet. (870) at 49



US006496867

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

(10) **Patent No.:** U
(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
6,381,646	B2	*	4/2002	Zhar	
6,400,722	B1	*	6/2002	Chu	

OTHER PUBLIC

Lee et al., “The Next Genration c teh Internet Protocol Version 6”, 1988, pp. 28–33.*
“Internet Engineering Task Force 791, Internet Protocol, Sep. 1981
“Internet Engineering Task Force 1853, IP in IP Tunneling, Oct. 19
“Internet Engineering Task Force 1701, Generic Routing Encapsulat 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.

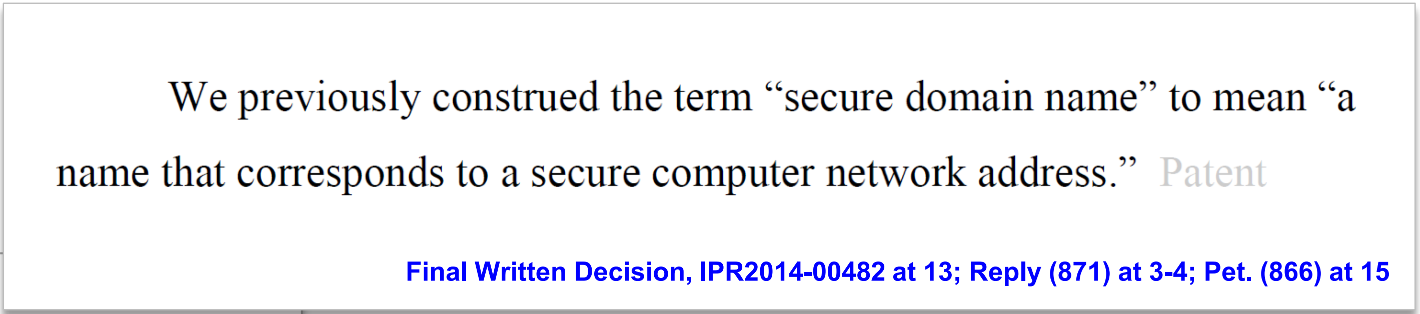
41 Claims, 17 Drawing Sheets

100
START
RECEIVE A REQUEST TO INITIATE A TUNNELING ASSOCIATION ON A FIRST NETWORK DEVICE
102
INFORM A TRUSTED-THIRD-PARTY NETWORK DEVICE OF THE REQUEST ON A PUBLIC NETWORK
104
ASSOCIATE A PUBLIC NETWORK ADDRESS FOR A SECOND NETWORK DEVICE ON THE TRUSTED-THIRD-PARTY NETWORK DEVICE
106
NEGOTIATE A FIRST PRIVATE NETWORK ADDRESS ON THE FIRST NETWORK DEVICE AND A SECOND PRIVATE NETWORK ADDRESS ON THE SECOND NETWORK DEVICE THROUGH THE PUBLIC NETWORK
108
END

Petitioner Apple Inc. - Exhibit 1007, p. 1

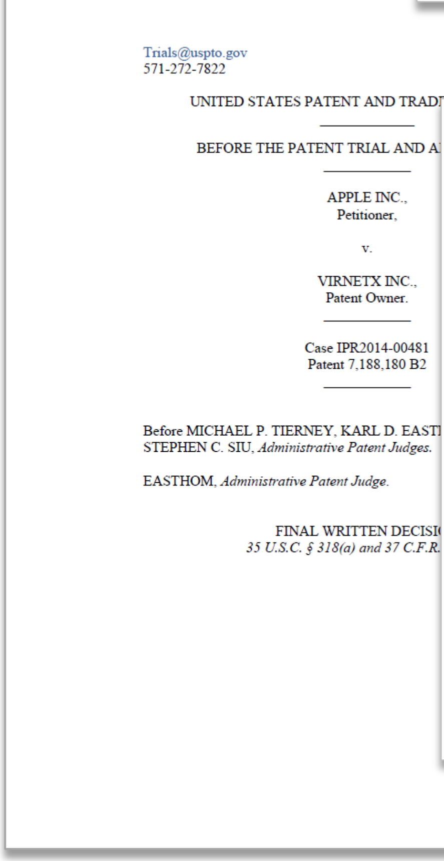
Final Written Decision in IPR2014-00481

"secure domain name"



We previously construed the term "secure domain name" to mean "a name that corresponds to a secure computer network address." Patent

Final Written Decision, IPR2014-00482 at 13; Reply (871) at 3-4; Pet. (866) at 15



Trials@uspto.gov
571-272-7822

Paper 35
Date: August 24, 2015

UNITED STATES PATENT AND TRAD

BEFORE THE PATENT TRIAL AND A

APPLE INC.,
Petitioner,

v.

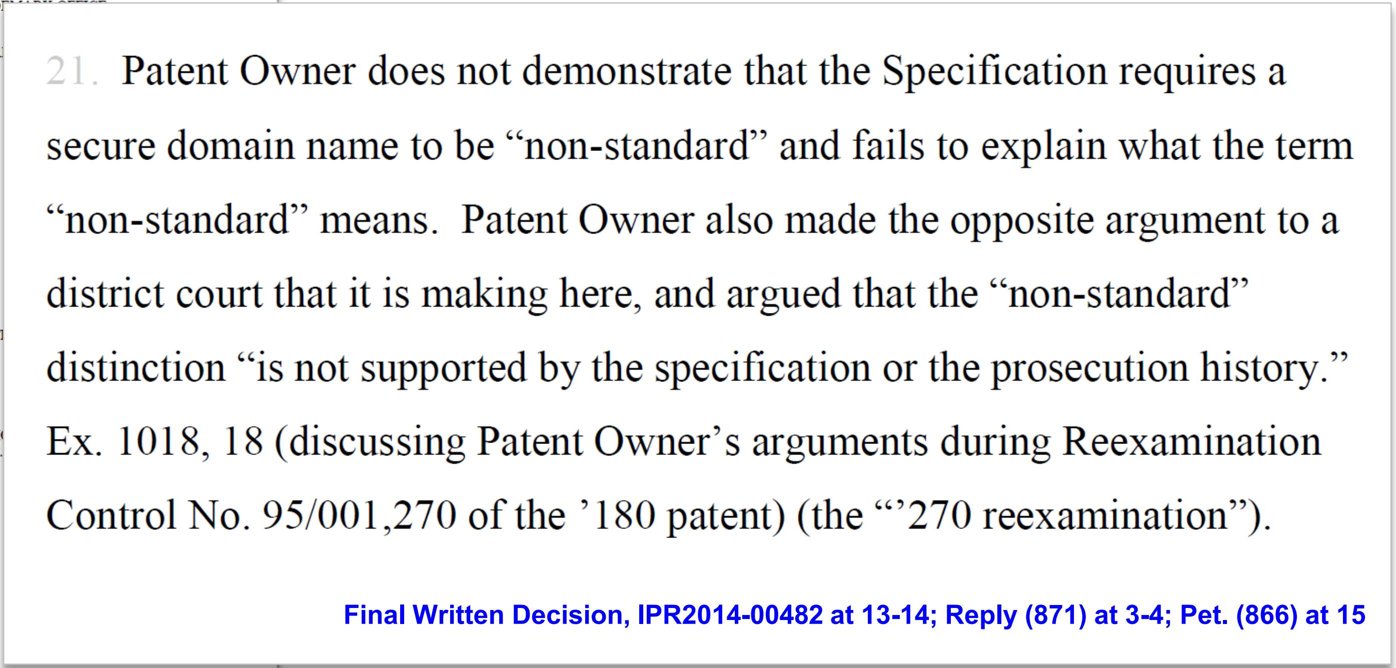
VIRNETX INC.,
Patent Owner.

Case IPR2014-00481
Patent 7,188,180 B2

Before MICHAEL P. TIERNEY, KARL D. EASTI
STEPHEN C. SIU, *Administrative Patent Judges.*

EASTHOM, *Administrative Patent Judge.*

FINAL WRITTEN DECISI
35 U.S.C. § 318(a) and 37 C.F.R.

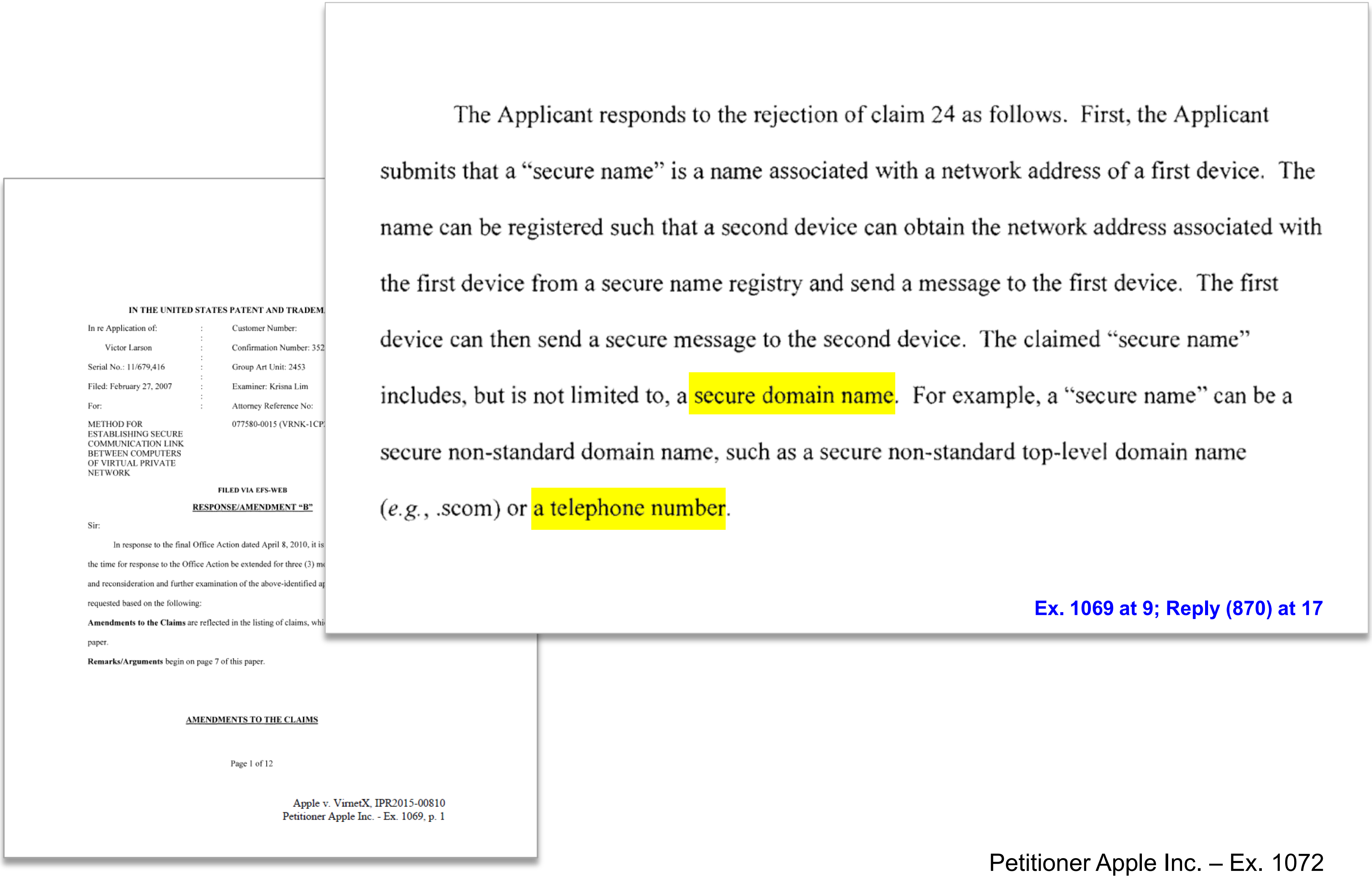


21. Patent Owner does not demonstrate that the Specification requires a secure domain name to be "non-standard" and fails to explain what the term "non-standard" means. Patent Owner also made the opposite argument to a district court that it is making here, and argued that the "non-standard" distinction "is not supported by the specification or the prosecution history." Ex. 1018, 18 (discussing Patent Owner's arguments during Reexamination Control No. 95/001,270 of the '180 patent) (the "'270 reexamination").

Final Written Decision, IPR2014-00482 at 13-14; Reply (871) at 3-4; Pet. (866) at 15

Patent Owner Admission

"secure domain name"



The Applicant responds to the rejection of claim 24 as follows. First, the Applicant submits that a "secure name" is a name associated with a network address of a first device. The name can be registered such that a second device can obtain the network address associated with the first device from a secure name registry and send a message to the first device. The first device can then send a secure message to the second device. The claimed "secure name" includes, but is not limited to, a secure domain name. For example, a "secure name" can be a secure non-standard domain name, such as a secure non-standard top-level domain name (*e.g.*, .scom) or a telephone number.

Ex. 1069 at 9; Reply (870) at 17

IN THE UNITED STATES PATENT AND TRADEM

In re Application of:	:	Customer Number:
Victor Larson	:	Confirmation Number: 352
Serial No.: 11/679,416	:	Group Art Unit: 2453
Filed: February 27, 2007	:	Examiner: Krisna Lim
For:	:	Attorney Reference No:
METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK		077580-0015 (VRNK-1CP

FILED VIA EFS-WEB

RESPONSE/AMENDMENT "B"

Sir:

In response to the final Office Action dated April 8, 2010, it is the time for response to the Office Action be extended for three (3) mo and reconsideration and further examination of the above-identified ap requested based on the following:

Amendments to the Claims are reflected in the listing of claims, whi paper.

Remarks/Arguments begin on page 7 of this paper.

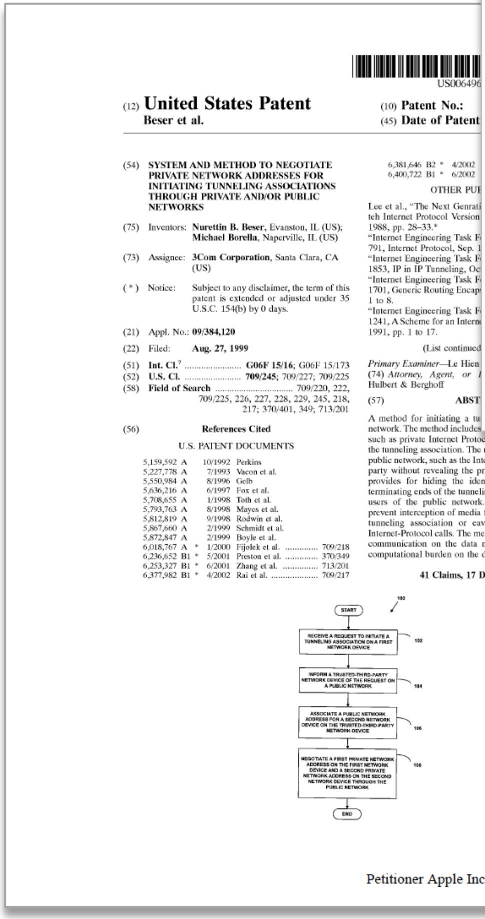
AMENDMENTS TO THE CLAIMS

Page 1 of 12

Apple v. VirnetX, IPR2015-00810
Petitioner Apple Inc. - Ex. 1069, p. 1

Beser and RFC 2401

“secure domain name”



US006496

(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

6,381,646 B2 * 4/2002
6,400,722 B1 * 6/2002

OTHER PUI

Lee et al., “The Next Genrati
teh Internet Protocol Version
1988, pp. 28–33.*
“Internet Engineering Task F
791, Internet Protocol, Sep. 1
“Internet Engineering Task F
1853, IP in IP Tunneling, Oc
“Internet Engineering Task F
1701, Generic Routing Encap
1 to 8.
“Internet Engineering Task F
1241, A Scheme for an Intern
1991, pp. 1 to 17.

(List continued

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

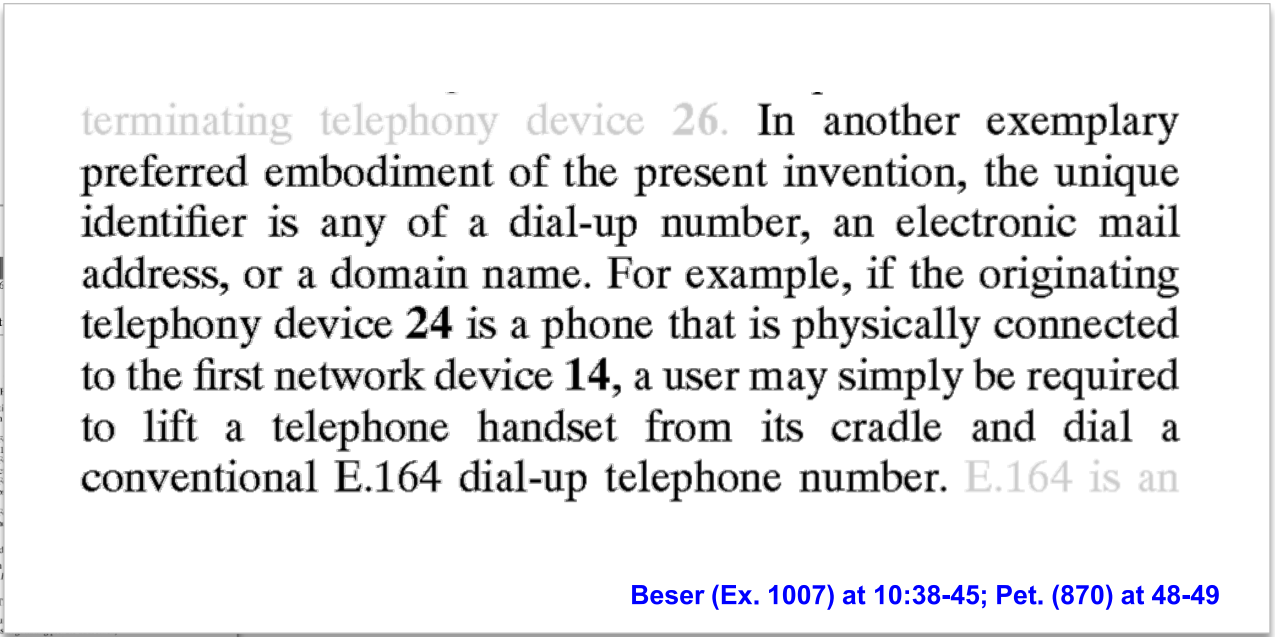
(57) ABST

A method for initiating a tu
network. The method includes
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

100
START
RECEIVE A REQUEST TO INITIATE A TUNNELING ASSOCIATION ON A FIRST NETWORK DEVICE
102
INFORM A TRUSTED-THIRD-PARTY NETWORK DEVICE OF THE REQUEST ON A PUBLIC NETWORK
104
ASSOCIATE A PUBLIC NETWORK ADDRESS FOR A SECOND NETWORK DEVICE ON THE TRUSTED-THIRD-PARTY NETWORK DEVICE
106
NEGOTIATE A FIRST PRIVATE NETWORK ADDRESS ON THE FIRST NETWORK DEVICE AND A SECOND PRIVATE NETWORK ADDRESS ON THE SECOND NETWORK DEVICE THROUGH THE PUBLIC NETWORK
108
END

Petitioner Apple Inc. - Exhibit 1007, p. 1



terminating telephony device 26. In another exemplary preferred embodiment of the present invention, the unique identifier is any of a dial-up number, an electronic mail address, or a domain name. For example, if the originating telephony device **24** is a phone that is physically connected to the first network device **14**, a user may simply be required to lift a telephone handset from its cradle and dial a conventional E.164 dial-up telephone number. E.164 is an

Beser (Ex. 1007) at 10:38-45; Pet. (870) at 48-49

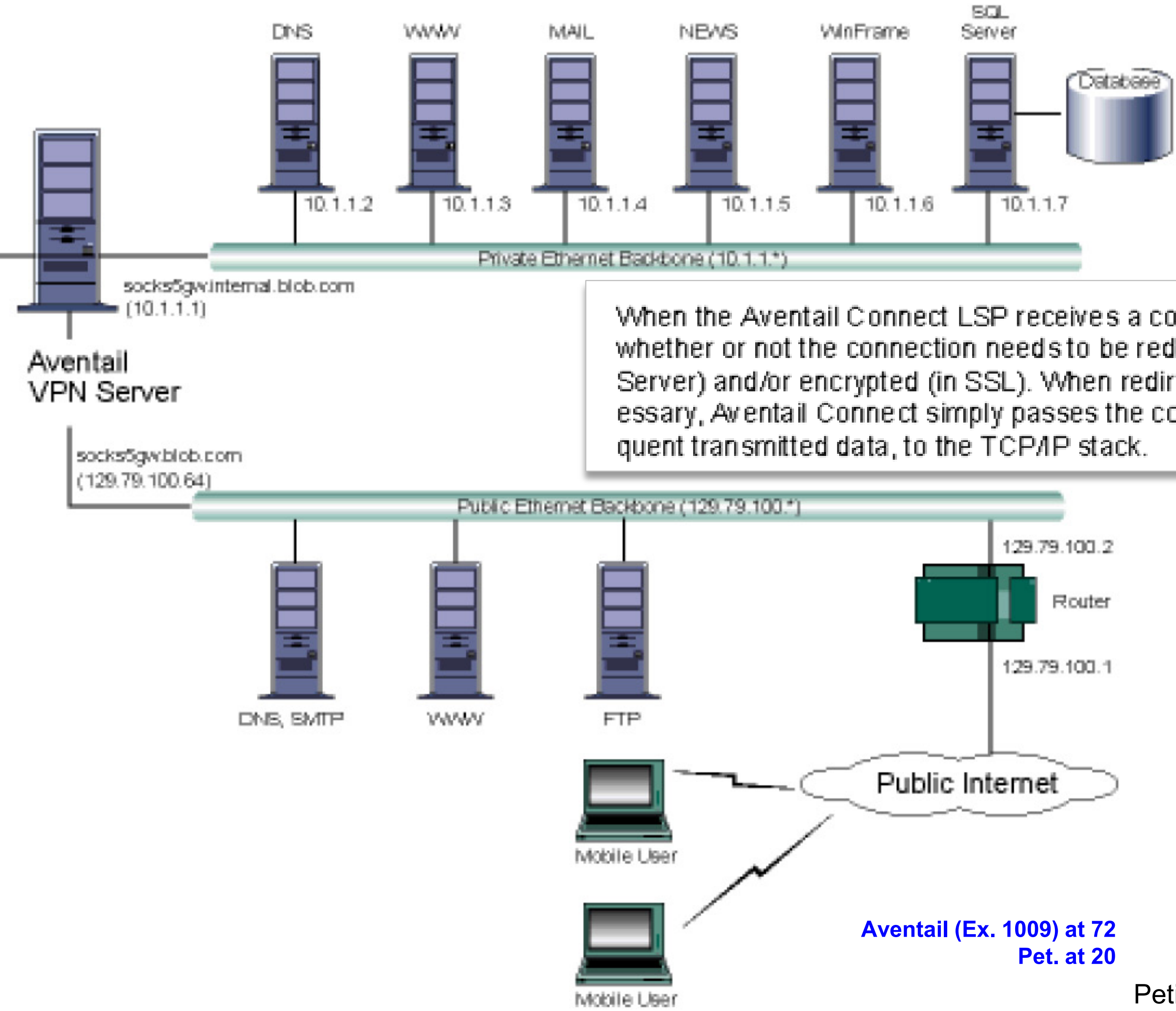
IPR2015-00871

Grounds

1. **Whether Claims 1-23 and 25-30 are obvious under 35 U.S.C. § 103 over Aventail (Ex. 1009), and RFC 2401 (Ex. 1008), and RFC 2543 (Ex. 1013)**

2. Whether Claim 24 is obvious under 35 U.S.C. § 103 over Aventail (Ex. 1009), and RFC 2401 (Ex. 1008), RFC 2543 (Ex. 1013), and Brand (Ex. 1012)

Grounds Based on Aventail and RFCs 2401 & 2543

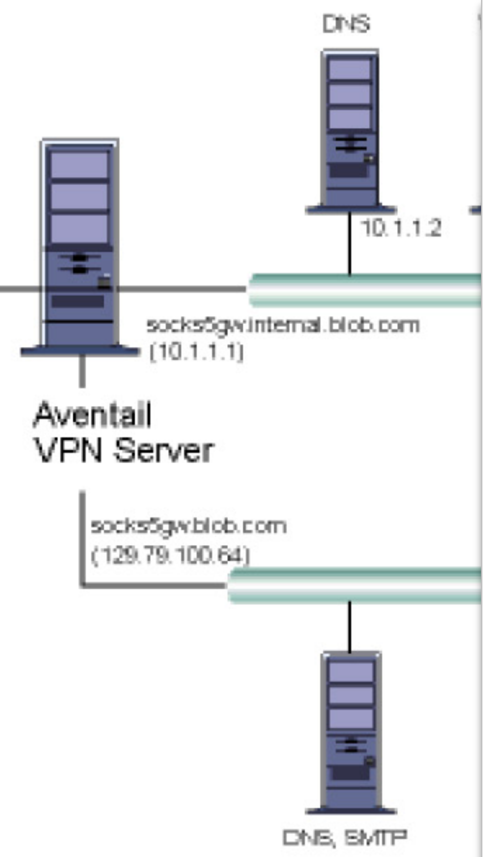


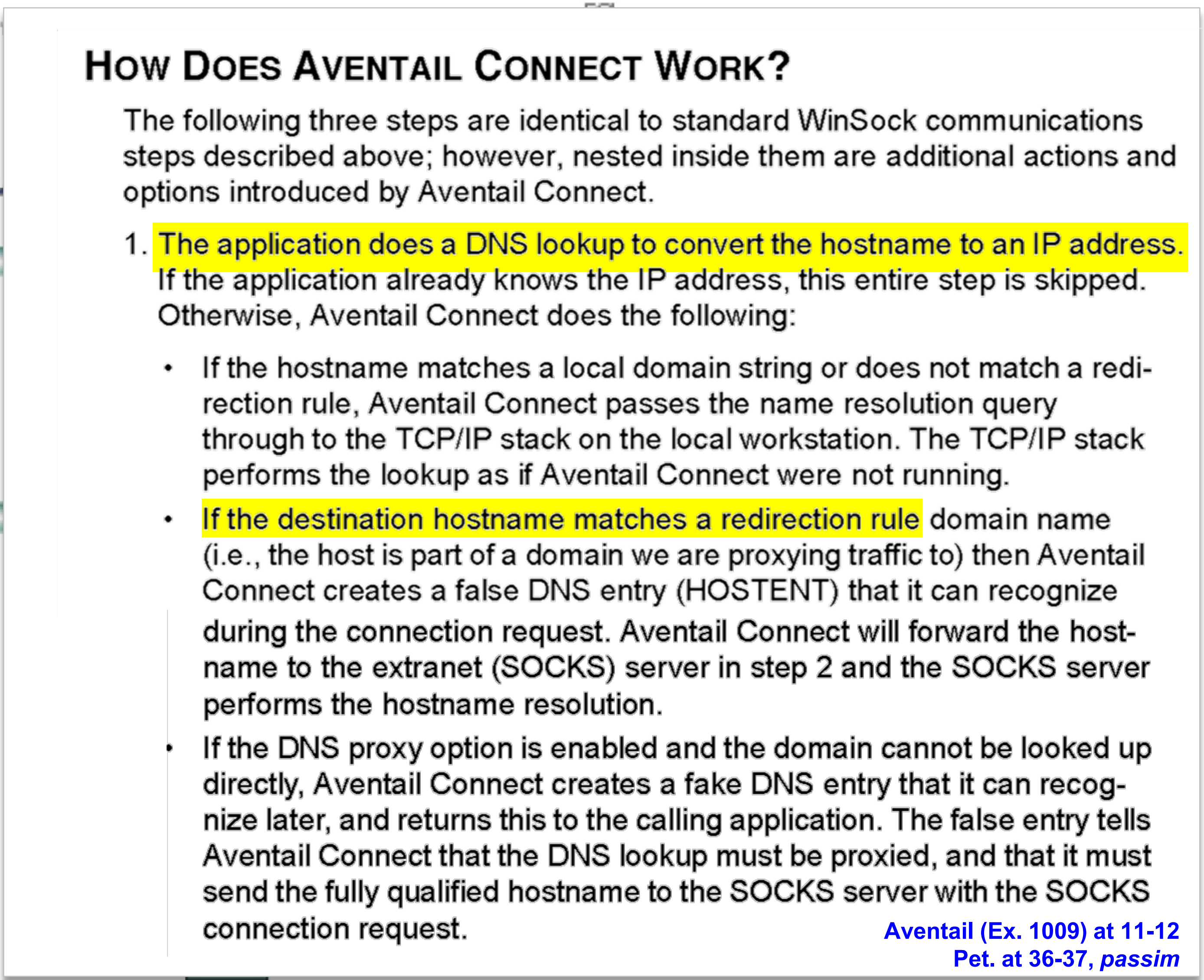
> When the Aventail Connect LSP receives a connection request, it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) and/or encrypted (in SSL). When redirection and encryption are not necessary, Aventail Connect simply passes the connection request, and any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

Aventail (Ex. 1009) at 10; Pet. at 22, 33

Aventail (Ex. 1009) at 72
Pet. at 20

Grounds Based on Aventail and RFCs 2401 & 2543





How Does Aventail Connect Work?

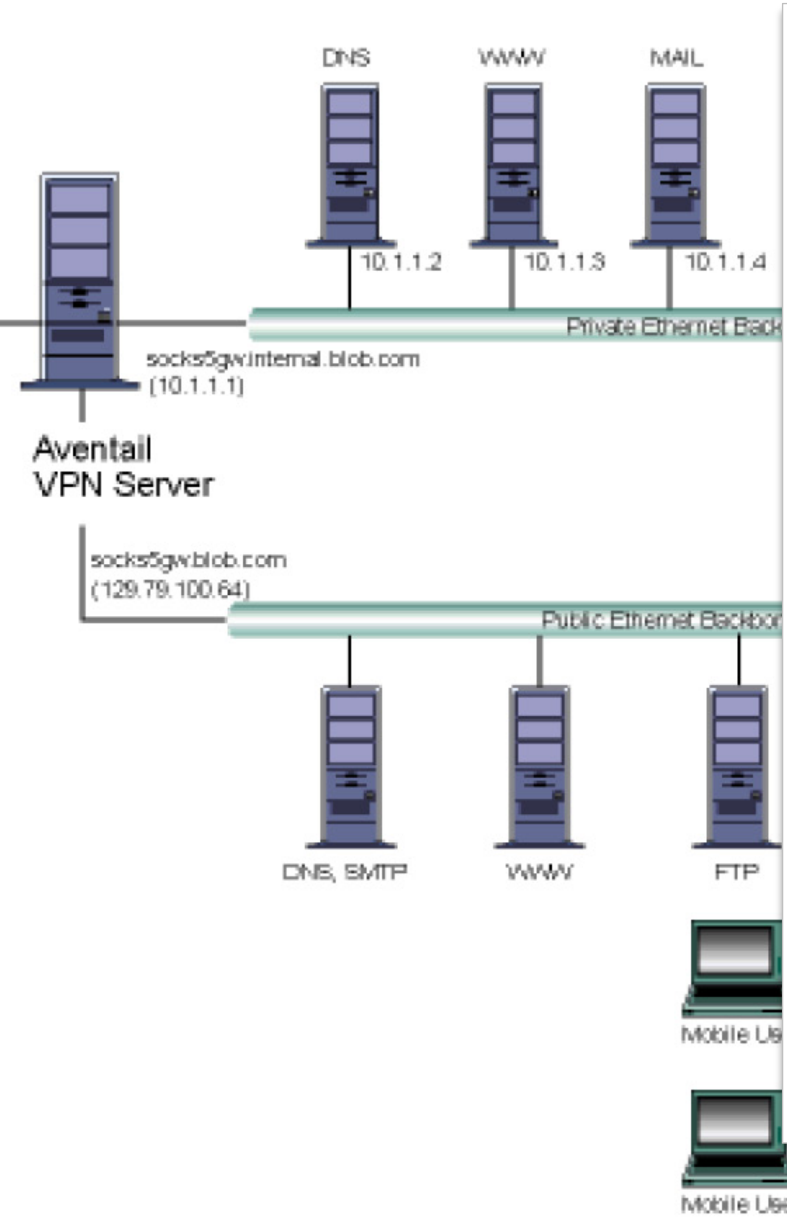
The following three steps are identical to standard WinSock communications steps described above; however, nested inside them are additional actions and options introduced by Aventail Connect.

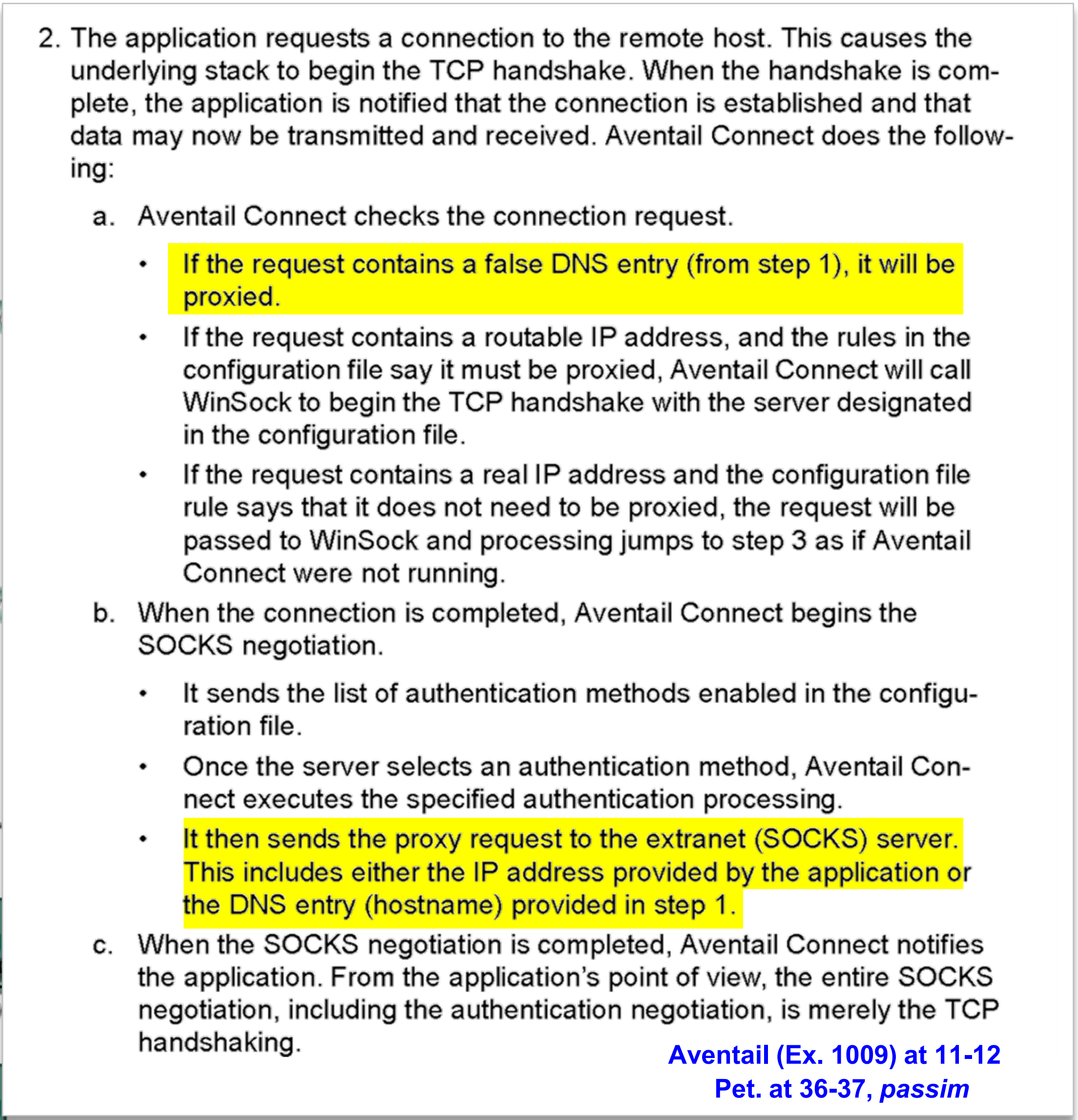
1. The application does a DNS lookup to convert the hostname to an IP address. If the application already knows the IP address, this entire step is skipped. Otherwise, Aventail Connect does the following:

   - 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 36-37, *passim*

Grounds Based on Aventail and RFCs 2401 & 2543





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 36-37, *passim*

IPR2015-00871
Aventail, RFC 2401, and RFC 2543 Issues

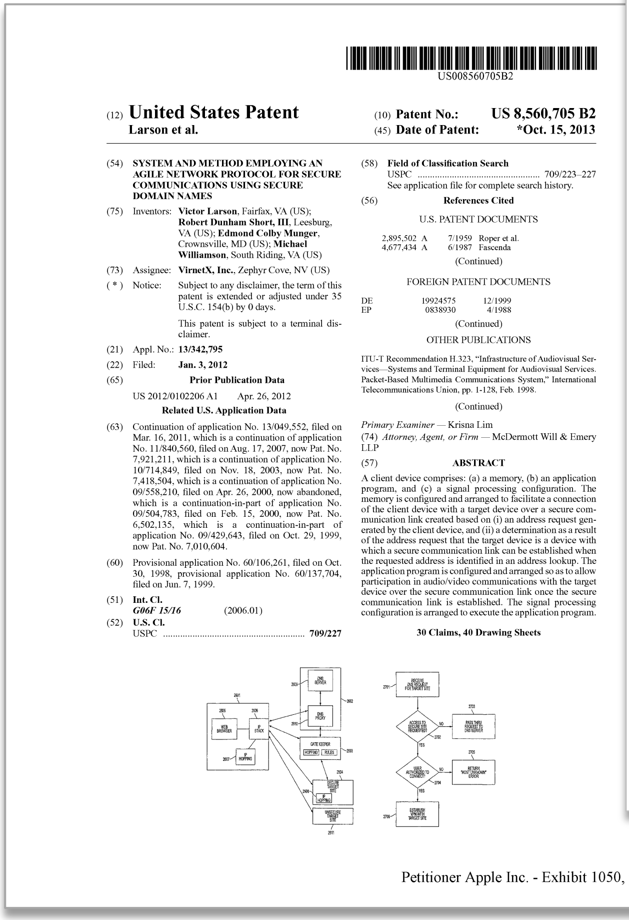
1. **Aventail, RFC 2401, and RFC 2543 Issues**

   A. **Aventail and the RFCs teach a "*Determination as a Result of the Request that the Target Device Is a Device with which a Secure Communication Link Can be Established" (claims 1, 16)***

   B. Aventail and the RFCs teach a "*Secure Communications Link*" between the Client and Target Devices *(claims 1, 16)* and a *"VPN" (claims 6, 21)*

’705 Patent, Claim 1

Aventail, RFC 2401, and RFC 2543 Issues



US008560705B2

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

(10) **Patent No.: US 8,560,705 B2**
(45) **Date of Patent: *Oct. 15, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/342,795**

(22) Filed: **Jan. 3, 2012**

(65) **Prior Publication Data**

US 2012/0102206 A1 Apr. 26, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,677,434	A	6/1987	Fascenda

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

ITU-T Recommendation H.323, “Infrastructure of Audiovisual Services—Systems and Terminal Equipment for Audiovisual Services. Packet-Based Multimedia Communications System,” International Telecommunications Union, pp. 1-128, Feb. 1998.

(Continued)

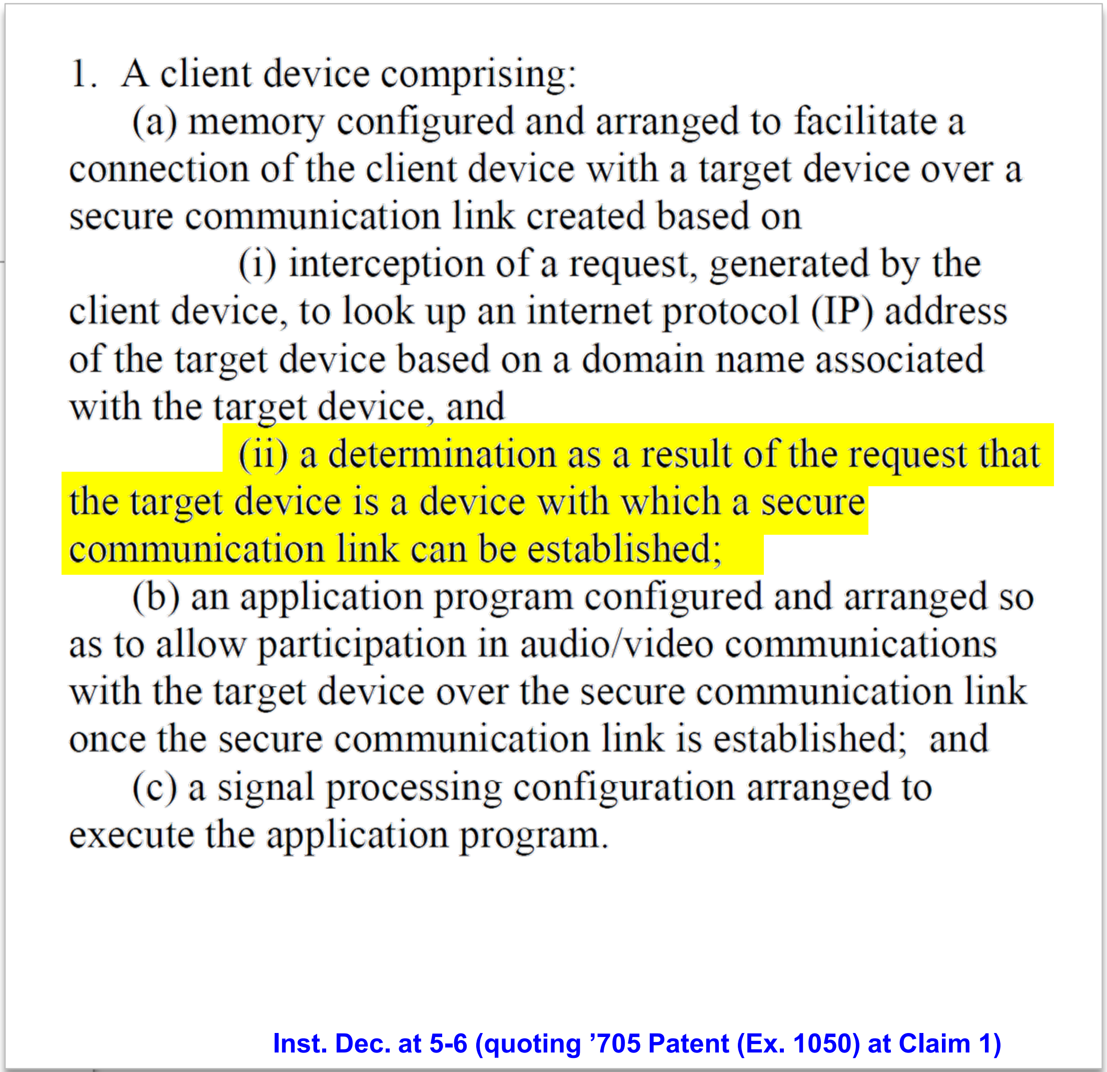
Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

A client device comprises: (a) a memory, (b) an application program, and (c) a signal processing configuration. The memory is configured and arranged to facilitate a connection of the client device with a target device over a secure communication link created based on (i) an address request generated by the client device, and (ii) a determination as a result of the address request that the target device is a device with which a secure communication link can be established when the requested address is identified in an address lookup. The application program is configured and arranged so as to allow participation in audio/video communications with the target device over the secure communication link once the secure communication link is established. The signal processing configuration is arranged to execute the application program.

30 Claims, 40 Drawing Sheets

Petitioner Apple Inc. - Exhibit 1050, p. 1



1. A client device comprising:

(a) memory configured and arranged to facilitate a connection of the client device with a target device over a secure communication link created based on

(i) interception of a request, generated by the client device, to look up an internet protocol (IP) address of the target device based on a domain name associated with the target device, and

(ii) a determination as a result of the request that the target device is a device with which a secure communication link can be established;

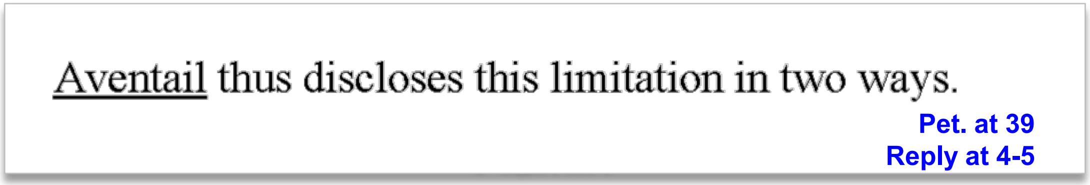
(b) an application program configured and arranged so as to allow participation in audio/video communications with the target device over the secure communication link once the secure communication link is established; and

(c) a signal processing configuration arranged to execute the application program.

Inst. Dec. at 5-6 (quoting ’705 Patent (Ex. 1050) at Claim 1)

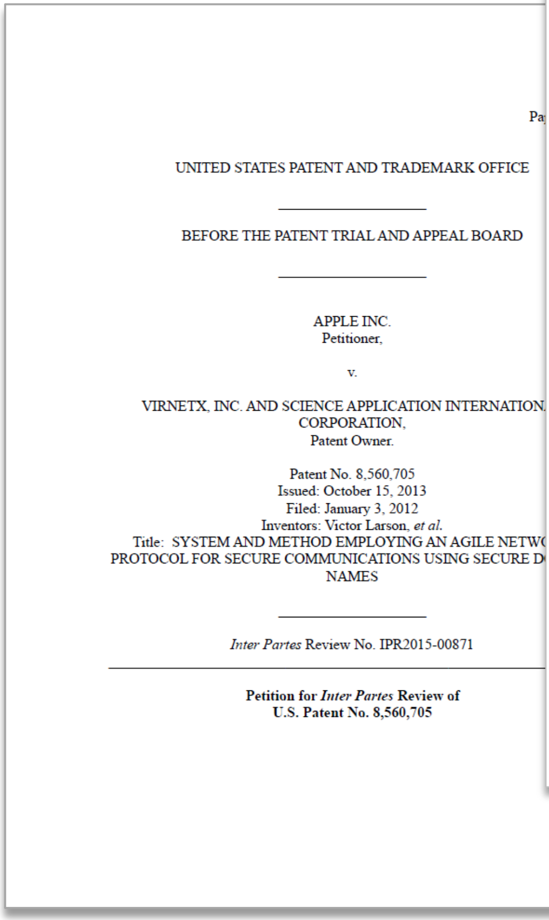
Grounds Based on Aventail and RFCs 2401 & 2543

"a determination as a result of the request"



Aventail thus discloses this limitation in two ways.

Pet. at 39
Reply at 4-5



Pa

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

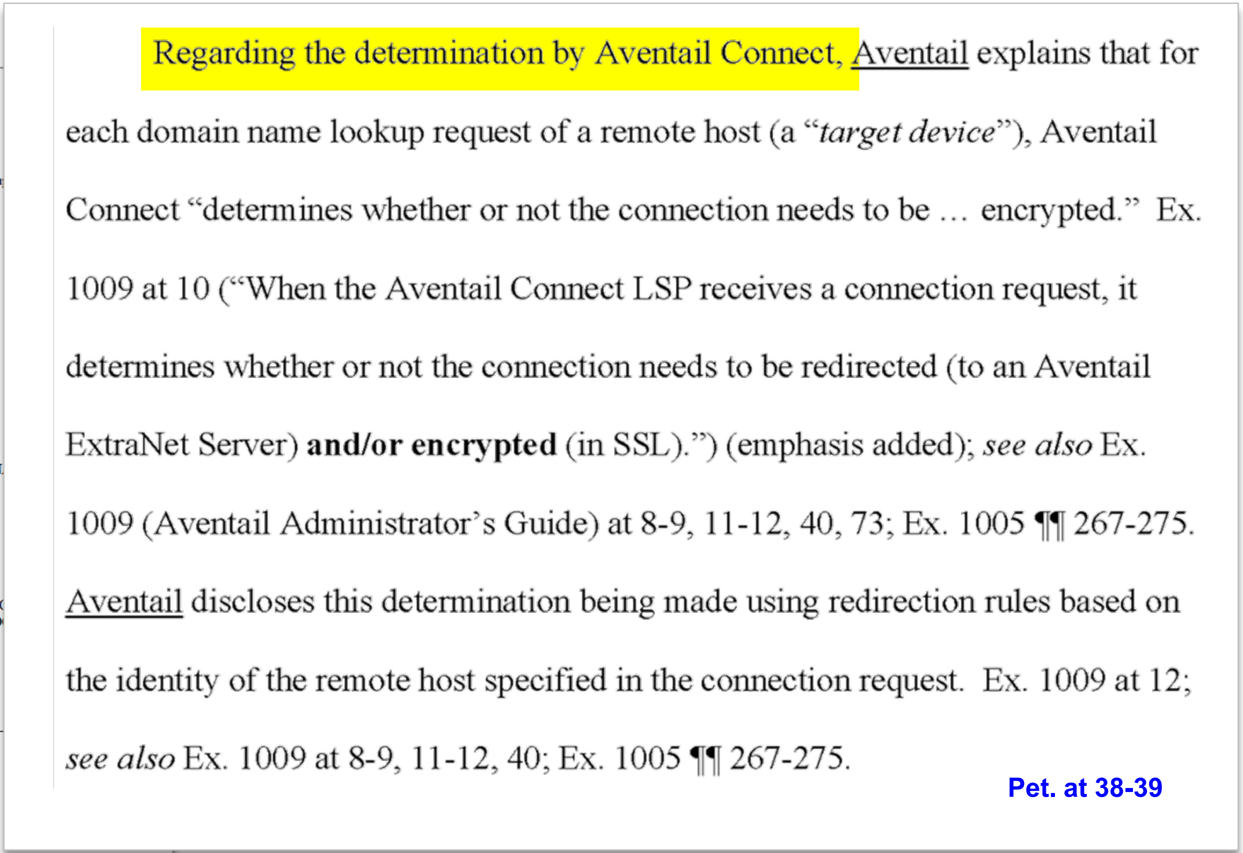
v.

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

Patent No. 8,560,705
Issued: October 15, 2013
Filed: January 3, 2012
Inventors: Victor Larson, *et al.*
Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETW
PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE D
NAMES

Inter Partes Review No. IPR2015-00871

Petition for *Inter Partes* Review of
U.S. Patent No. 8,560,705

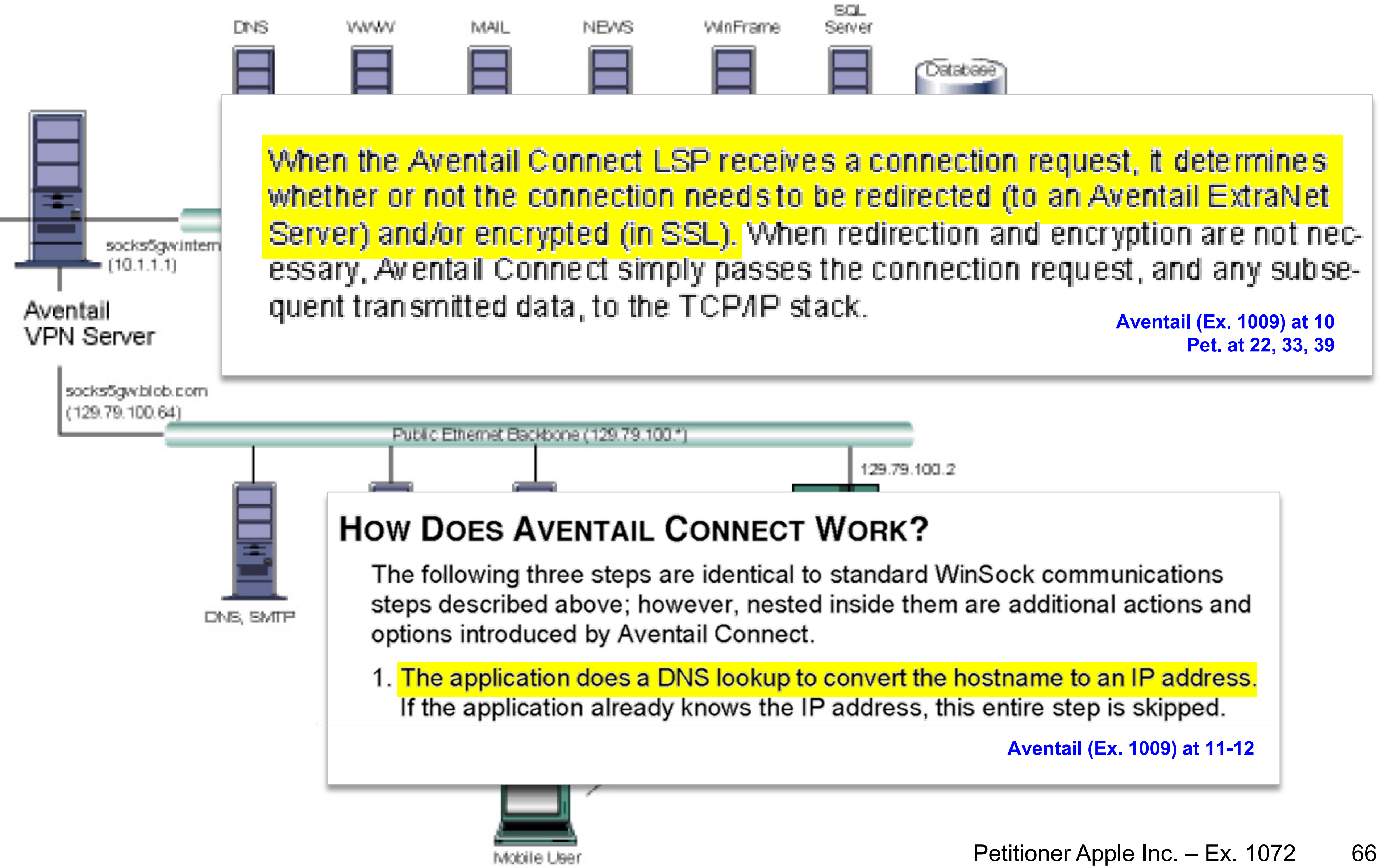


Regarding the determination by Aventail Connect, Aventail explains that for each domain name lookup request of a remote host (a "*target device*"), Aventail Connect "determines whether or not the connection needs to be … encrypted." Ex. 1009 at 10 ("When the Aventail Connect LSP receives a connection request, it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) **and/or encrypted** (in SSL).") (emphasis added); *see also* Ex. 1009 (Aventail Administrator's Guide) at 8-9, 11-12, 40, 73; Ex. 1005 ¶¶ 267-275. Aventail discloses this determination being made using redirection rules based on the identity of the remote host specified in the connection request. Ex. 1009 at 12; *see also* Ex. 1009 at 8-9, 11-12, 40; Ex. 1005 ¶¶ 267-275.

Pet. at 38-39

Grounds Based on Aventail and RFCs 2401 & 2543

"a determination as a result of the request"


DNS
WWW
MAIL
NEWS
WinFrame
SQL Server
Database
socks5gw.intern (10.1.1.1)
Aventail VPN Server
socks5gw.blob.com (129.79.100.64)
Public Ethernet Backbone (129.79.100.*)
129.79.100.2
DNS, SMTP
Mobile User

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 22, 33, 39

How Does Aventail Connect Work?

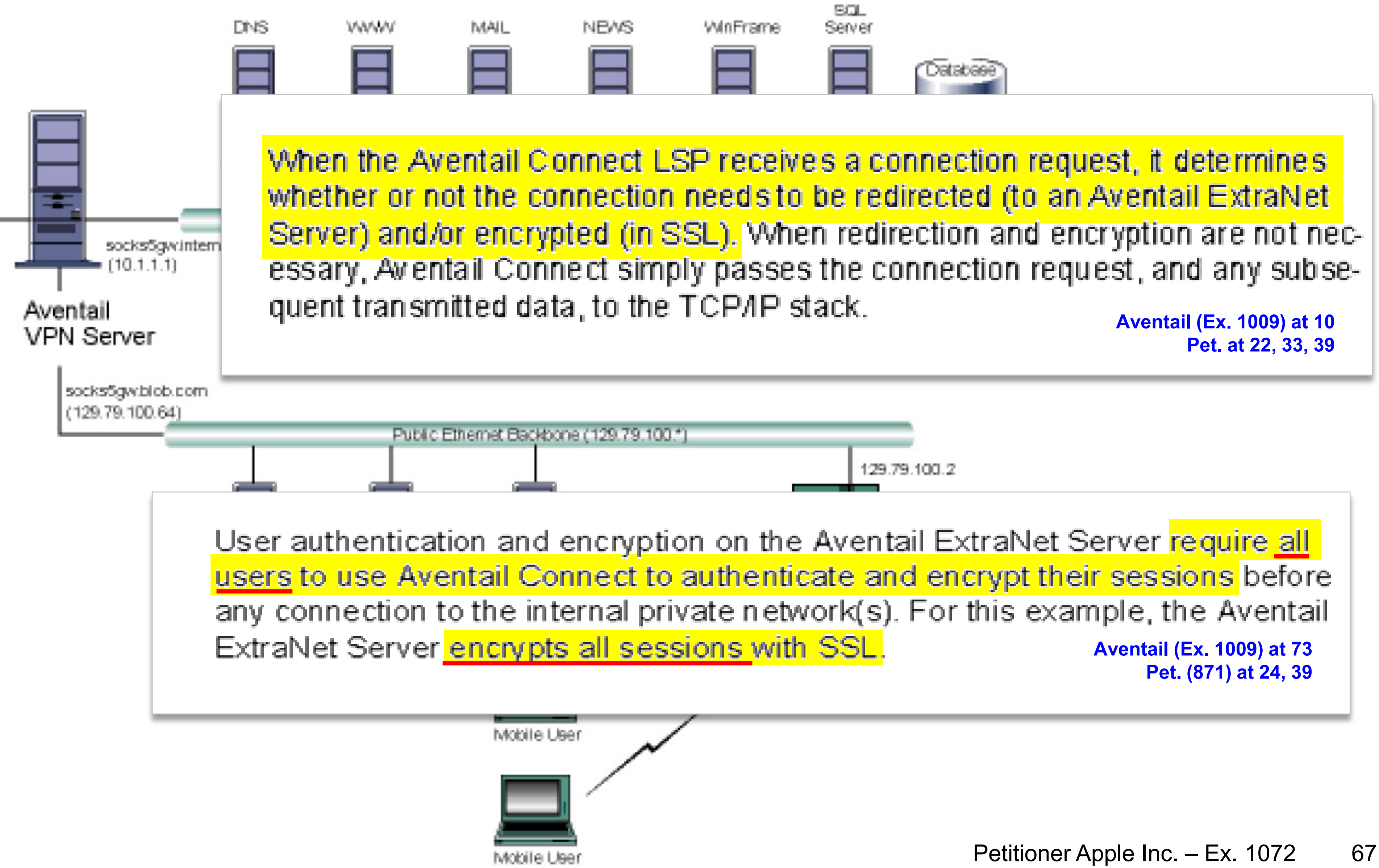
The following three steps are identical to standard WinSock communications steps described above; however, nested inside them are additional actions and options introduced by Aventail Connect.

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 RFCs 2401 & 2543

"a determination as a result of the request"



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.

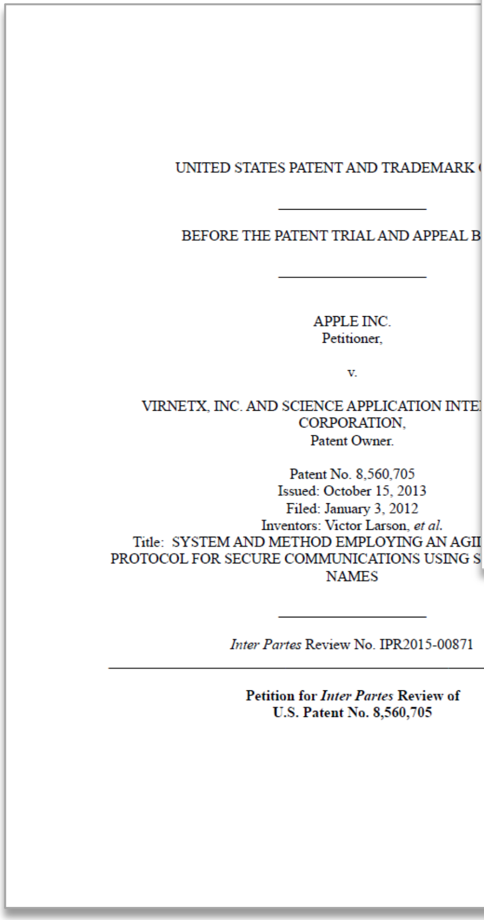
Aventail (Ex. 1009) at 10
Pet. at 22, 33, 39

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. (871) at 24, 39

Grounds Based on Aventail and RFCs 2401 & 2543

"a determination as a result of the request"



UNITED STATES PATENT AND TRADEMARK

BEFORE THE PATENT TRIAL AND APPEAL B

APPLE INC.
Petitioner,

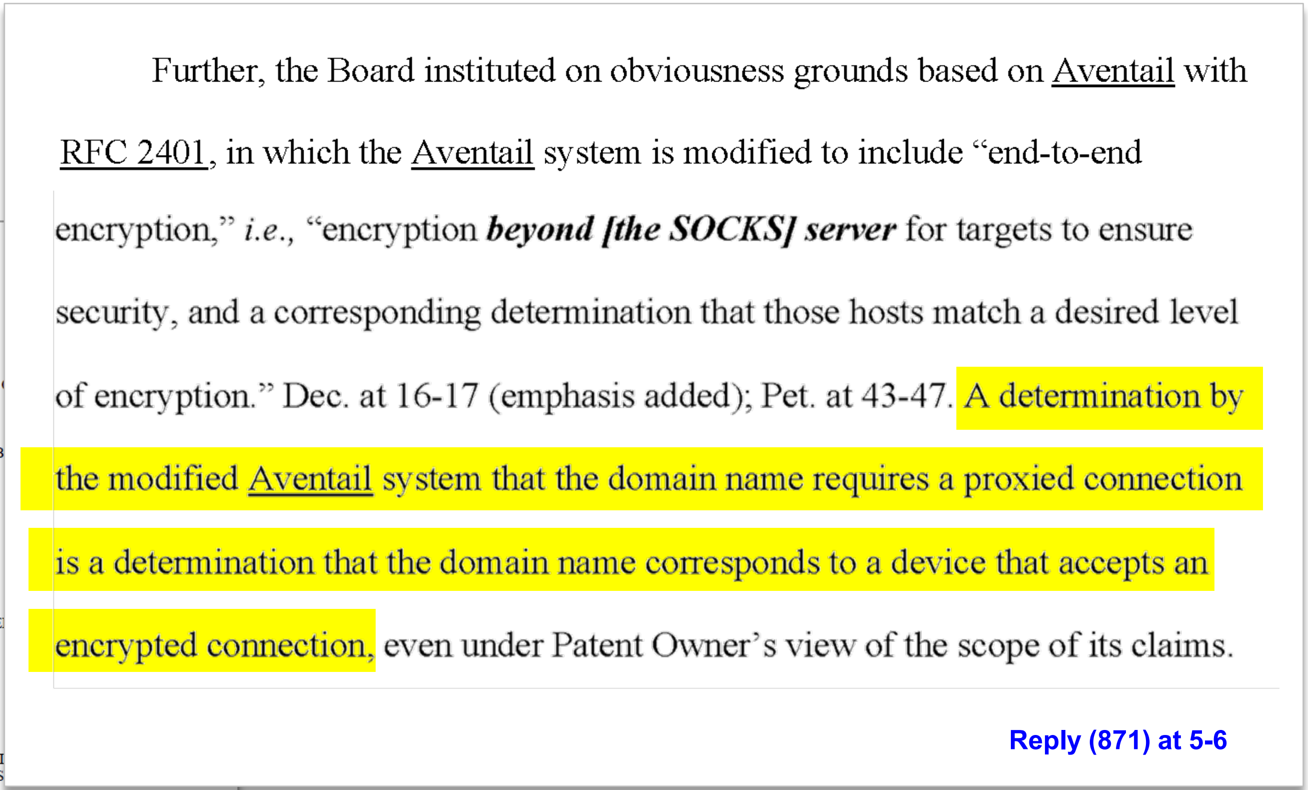
v.

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

Patent No. 8,560,705
Issued: October 15, 2013
Filed: January 3, 2012
Inventors: Victor Larson, *et al.*
Title: SYSTEM AND METHOD EMPLOYING AN AGIL
PROTOCOL FOR SECURE COMMUNICATIONS USING S
NAMES

Inter Partes Review No. IPR2015-00871

Petition for *Inter Partes* Review of
U.S. Patent No. 8,560,705

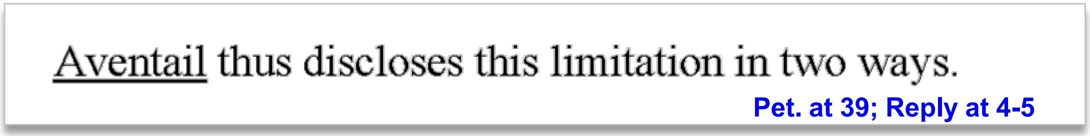


Further, the Board instituted on obviousness grounds based on Aventail with RFC 2401, in which the Aventail system is modified to include "end-to-end encryption," *i.e.*, "encryption ***beyond [the SOCKS] server*** for targets to ensure security, and a corresponding determination that those hosts match a desired level of encryption." Dec. at 16-17 (emphasis added); Pet. at 43-47. A determination by the modified Aventail system that the domain name requires a proxied connection is a determination that the domain name corresponds to a device that accepts an encrypted connection, even under Patent Owner's view of the scope of its claims.

Reply (871) at 5-6

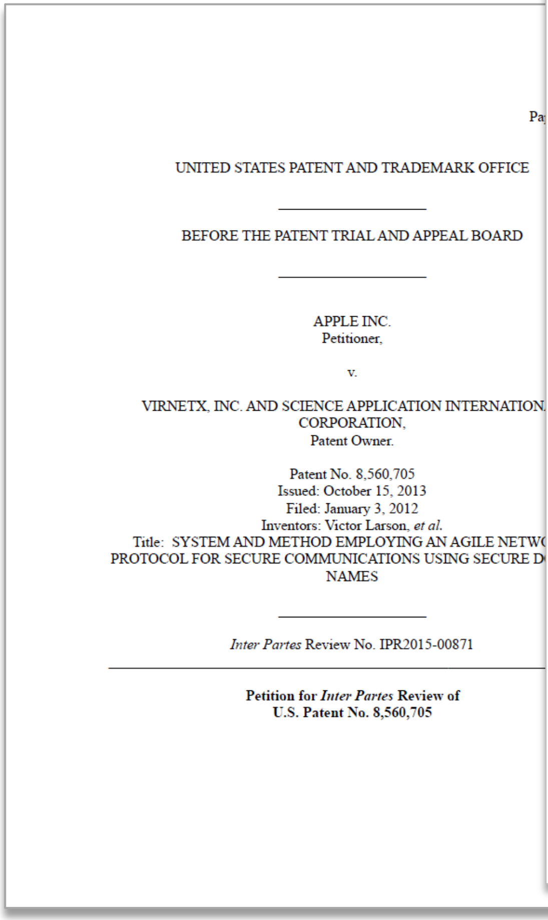
Grounds Based on Aventail and RFCs 2401 & 2543

"a determination as a result of the request"



Aventail thus discloses this limitation in two ways.

Pet. at 39; Reply at 4-5



Pa

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

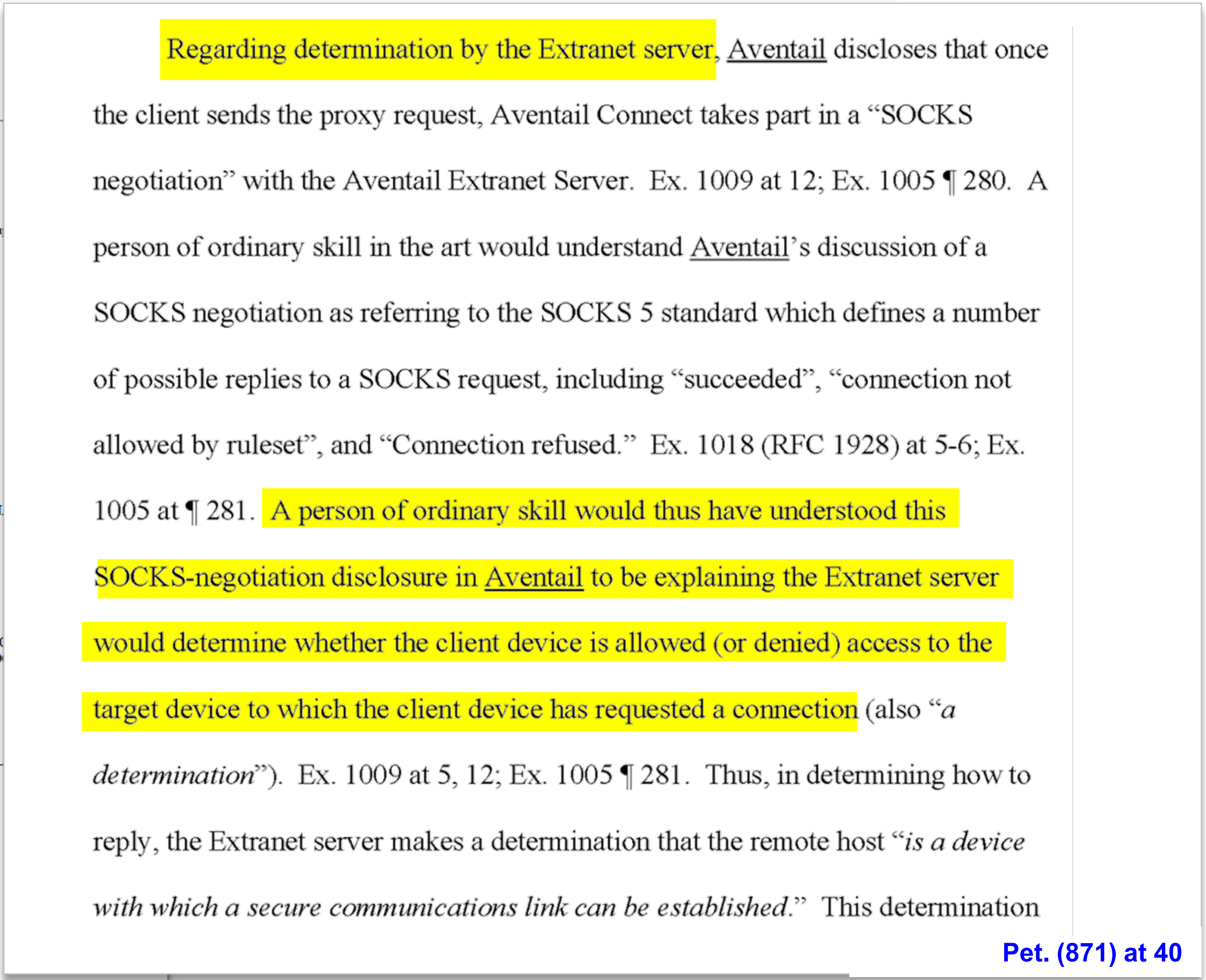
v.

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

Patent No. 8,560,705
Issued: October 15, 2013
Filed: January 3, 2012
Inventors: Victor Larson, *et al.*
Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETW
PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE D
NAMES

Inter Partes Review No. IPR2015-00871

Petition for *Inter Partes* Review of
U.S. Patent No. 8,560,705

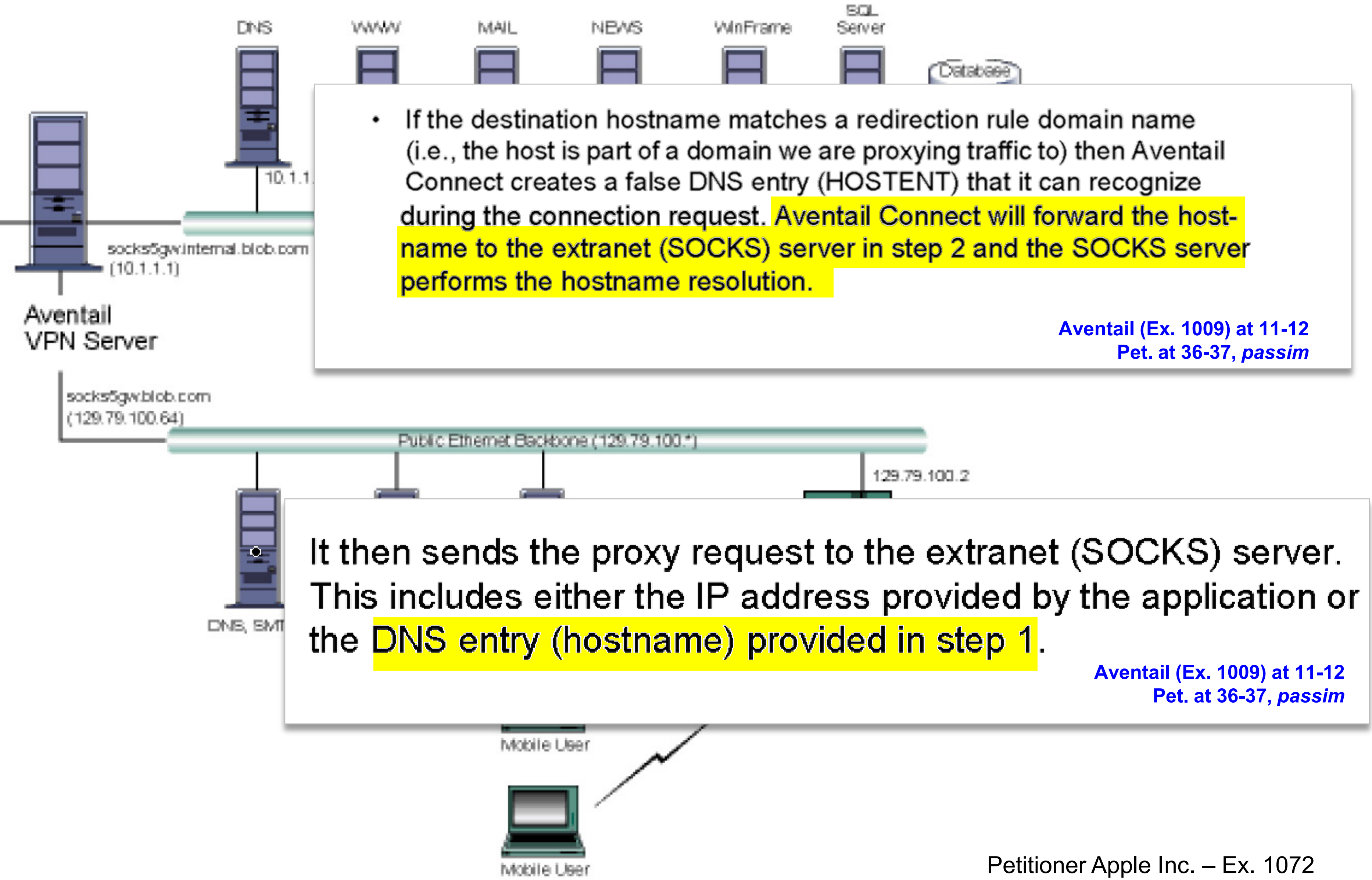


Regarding determination by the Extranet server, Aventail discloses that once the client sends the proxy request, Aventail Connect takes part in a "SOCKS negotiation" with the Aventail Extranet Server. Ex. 1009 at 12; Ex. 1005 ¶ 280. A person of ordinary skill in the art would understand Aventail's discussion of a SOCKS negotiation as referring to the SOCKS 5 standard which defines a number of possible replies to a SOCKS request, including "succeeded", "connection not allowed by ruleset", and "Connection refused." Ex. 1018 (RFC 1928) at 5-6; Ex. 1005 at ¶ 281. A person of ordinary skill would thus have understood this SOCKS-negotiation disclosure in Aventail to be explaining the Extranet server would determine whether the client device is allowed (or denied) access to the target device to which the client device has requested a connection (also "*a determination*"). Ex. 1009 at 5, 12; Ex. 1005 ¶ 281. Thus, in determining how to reply, the Extranet server makes a determination that the remote host "*is a device with which a secure communications link can be established.*" This determination

Pet. (871) at 40

Grounds Based on Aventail and RFCs 2401 & 2543

“a determination as a result of the request”


DNS
WWW
MAIL
NEWS
WinFrame
SQL Server
Database
10.1.1.
socks5gw.internal.blob.com (10.1.1.1)
Aventail VPN Server
socks5gw.blob.com (129.79.100.64)
Public Ethernet Backbone (129.79.100.*)
129.79.100.2
DNS, SMT
Mobile User
Mobile User

- 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 host-name to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution.

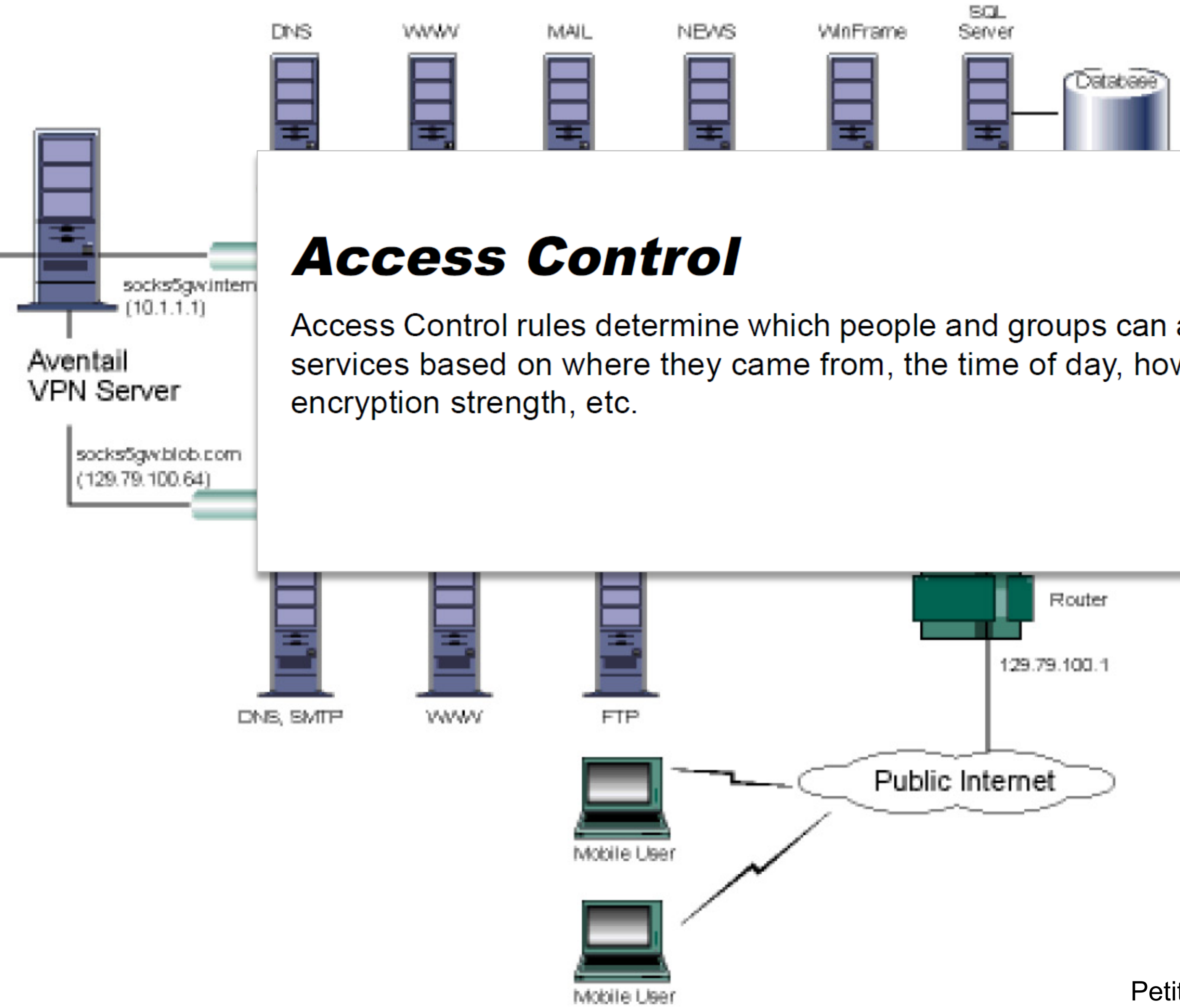
Aventail (Ex. 1009) at 11-12
Pet. at 36-37, *passim*

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 36-37, *passim*

Grounds Based on Aventail and RFCs 2401 & 2543

"a determination as a result of the request"



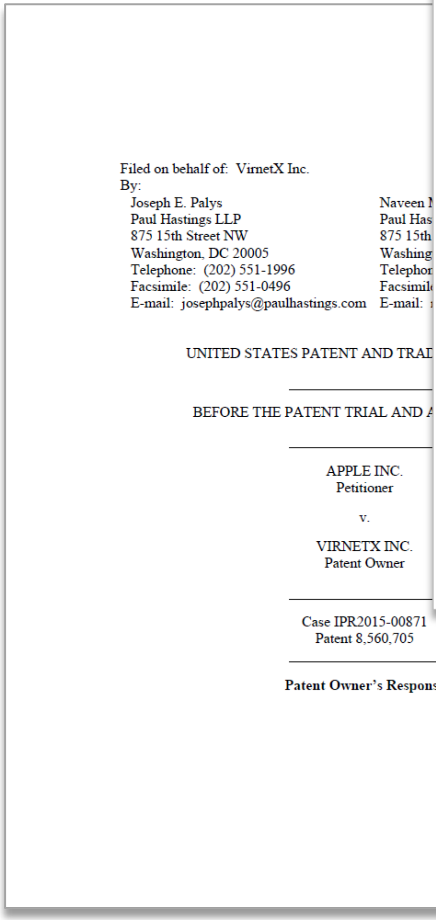
Access Control

Access Control rules determine which people and groups can access what machines and services based on where they came from, the time of day, how they authenticated, and encryption strength, etc.

Aventail (Ex. 1011) at 19
Pet. at 19; Reply at 8-9

Patent Owner Assertion

“a determination as a result of the request”



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 M
Paul Has
875 15th
Washing
Telephon
Facsimile
E-mail:

UNITED STATES PATENT AND TRAD

BEFORE THE PATENT TRIAL AND A

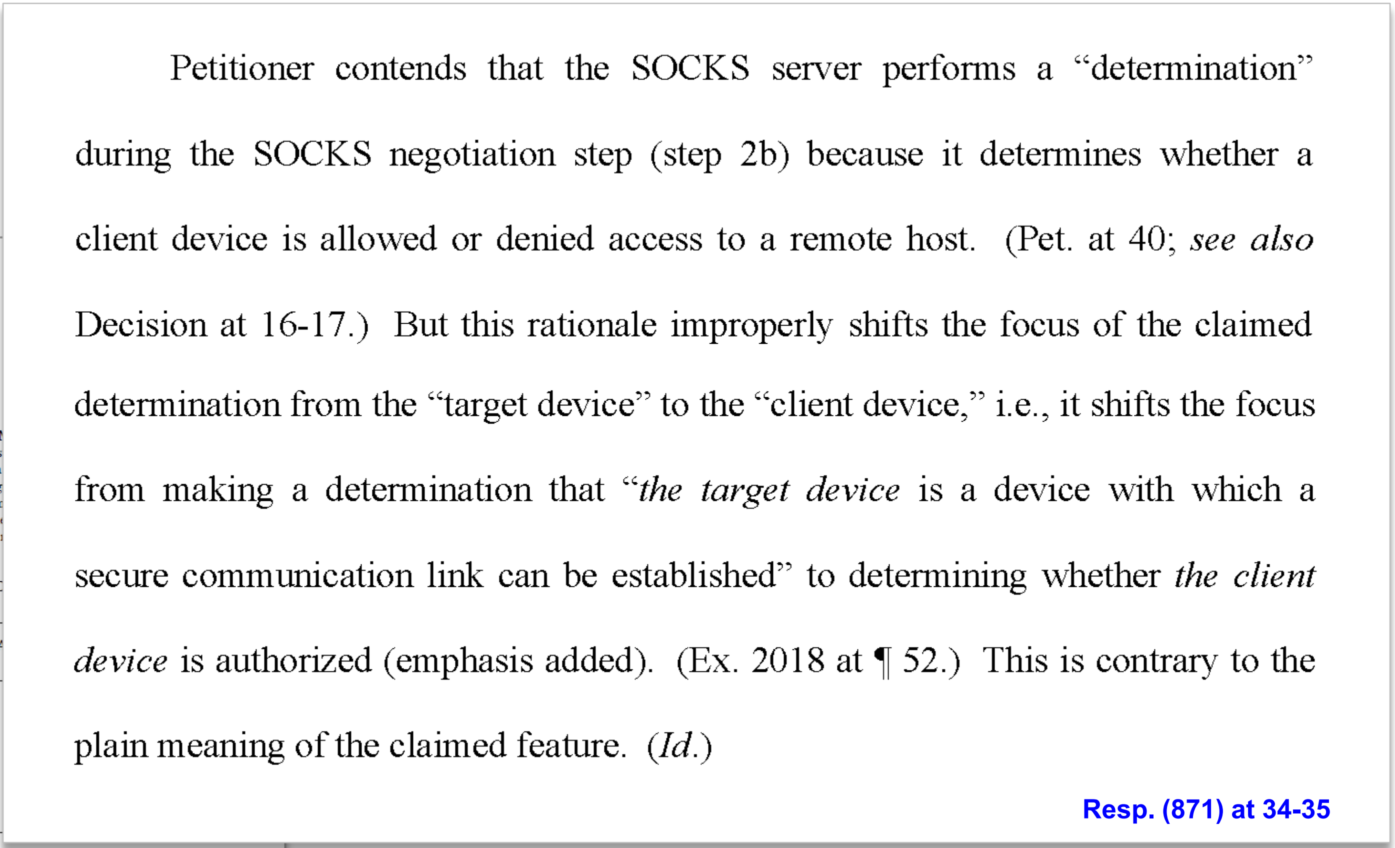
APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2015-00871
Patent 8,560,705

Patent Owner’s Response

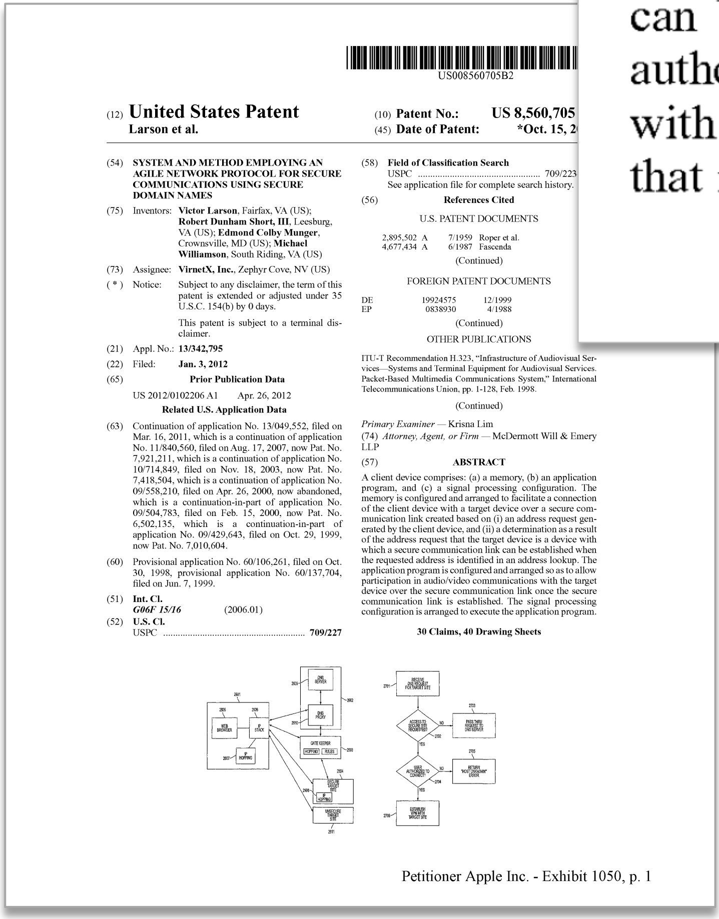


Petitioner contends that the SOCKS server performs a “determination” during the SOCKS negotiation step (step 2b) because it determines whether a client device is allowed or denied access to a remote host. (Pet. at 40; *see also* Decision at 16-17.) But this rationale improperly shifts the focus of the claimed determination from the “target device” to the “client device,” i.e., it shifts the focus from making a determination that “*the target device* is a device with which a secure communication link can be established” to determining whether *the client device* is authorized (emphasis added). (Ex. 2018 at ¶ 52.) This is contrary to the plain meaning of the claimed feature. (*Id.*)

Resp. (871) at 34-35

’705 Patent, Claim 1

“a determination as a result of the request”



US008560705B2

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

(10) **Patent No.: US 8,560,705**
(45) **Date of Patent: *Oct. 15, 2**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/342,795**

(22) Filed: **Jan. 3, 2012**

(65) **Prior Publication Data**

US 2012/0102206 A1 Apr. 26, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,677,434	A	6/1987	Fascenda

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

ITU-T Recommendation H.323, “Infrastructure of Audiovisual Services—Systems and Terminal Equipment for Audiovisual Services. Packet-Based Multimedia Communications System,” International Telecommunications Union, pp. 1-128, Feb. 1998.

(Continued)

Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

A client device comprises: (a) a memory, (b) an application program, and (c) a signal processing configuration. The memory is configured and arranged to facilitate a connection of the client device with a target device over a secure communication link created based on (i) an address request generated by the client device, and (ii) a determination as a result of the address request that the target device is a device with which a secure communication link can be established when the requested address is identified in an address lookup. The application program is configured and arranged so as to allow participation in audio/video communications with the target device over the secure communication link once the secure communication link is established. The signal processing configuration is arranged to execute the application program.

30 Claims, 40 Drawing Sheets

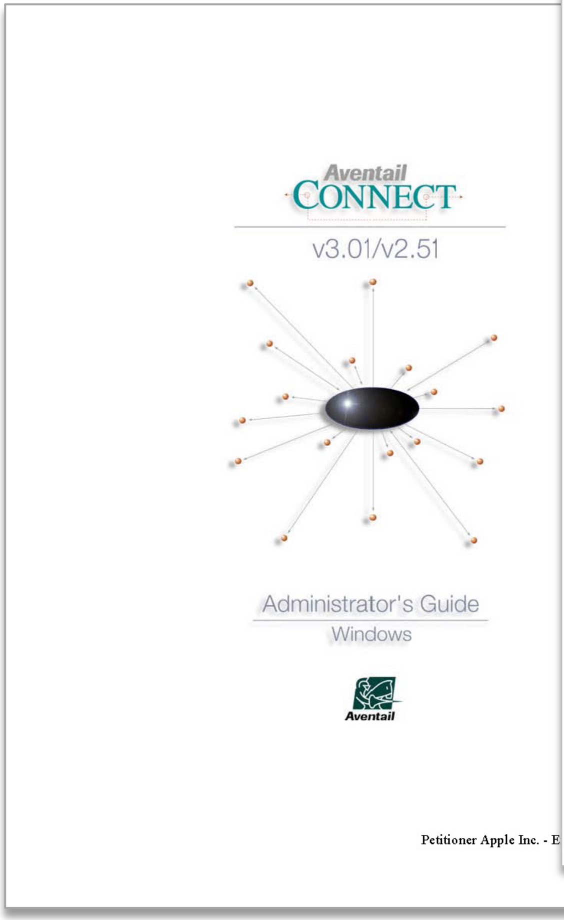
Petitioner Apple Inc. - Exhibit 1050, p. 1

In step **2702**, if access to a secure host was requested, then in step **2704** a further check is made to determine whether the user is authorized to connect to the secure host. Such a check can be made with reference to an internally stored list of authorized IP addresses, or can be made by communicating with gatekeeper **2603** (e.g., over an “administrative” VPN that is secure). It will be appreciated that different levels of

’705 Patent (Ex. 1050) at 40:57-63; Reply at 8

Grounds Based on Aventail and RFCs 2401 & 2543

"a determination as a result of the request"



Aventail CONNECT

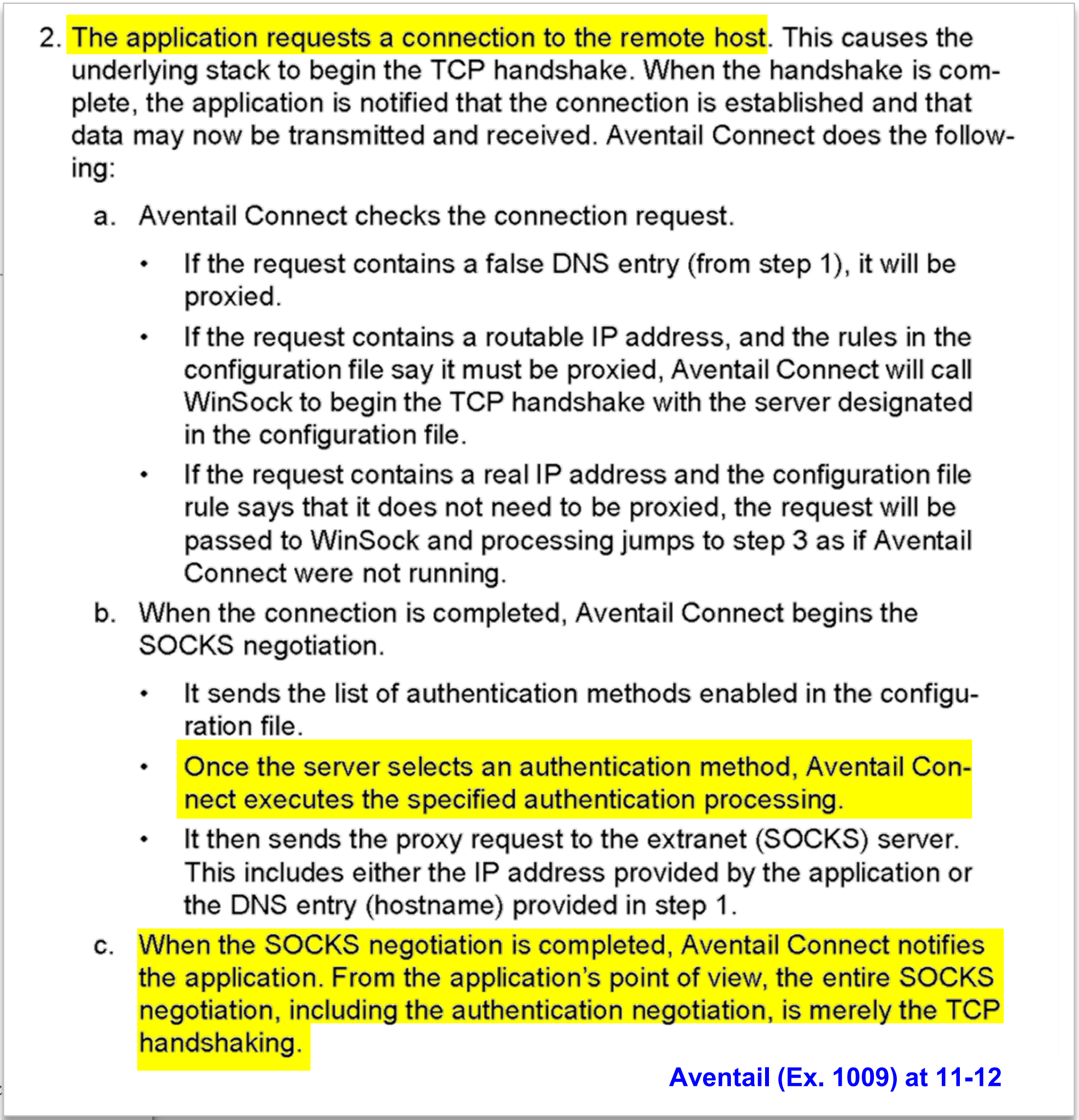
v3.01/v2.51

Administrator's Guide

Windows

Aventail

Petitioner Apple Inc. - E



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

IPR2015-00871

Aventail, RFC 2401, and RFC 2543 Issues

1. **Aventail, RFC 2401, and RFC 2543 Issues**

   A. Aventail and the RFCs teach a "*Determination as a Result of the Request that the Target Device Is a Device with which a Secure Communication Link Can be Established*" *(claims 1, 16)*

   B. **Aventail and the RFCs teach a "*Secure Communications Link*" between the Client and Target Devices *(claims 1, 16)* and a *"VPN" (claims 6, 21)***

"Secure Communication Link" and *"[VPN] Link"*

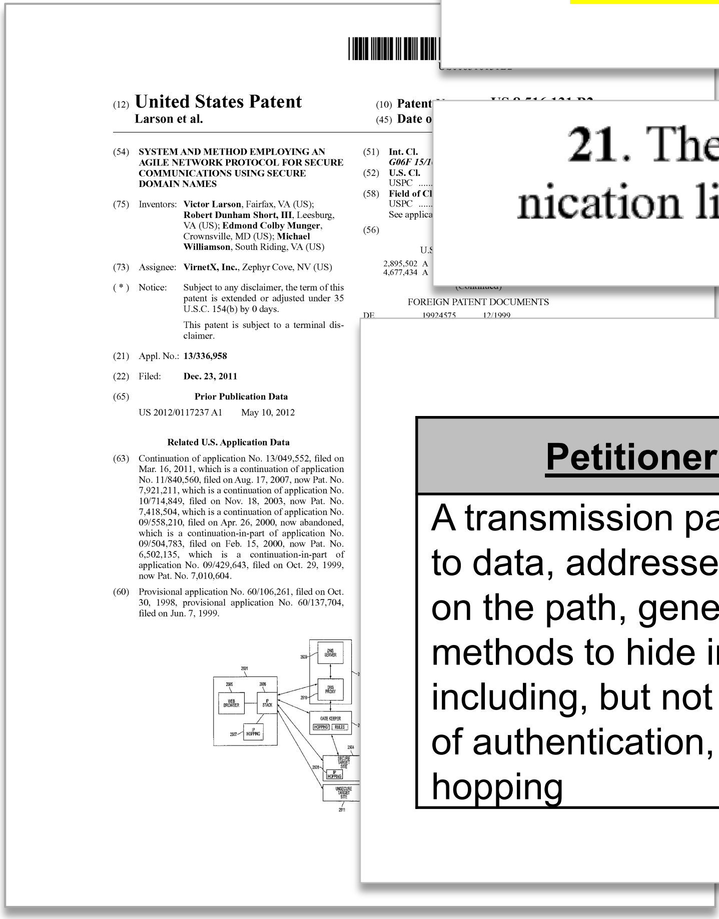
16. A method executed by a client device for communicating with a target device, the method comprising:

(a) facilitating a connection with the target device over a secure communication link created based on (i) inter-

'705 Patent (Ex. 1050) at Claim 16

21. The method of claim **16**, wherein the secure communication link is a virtual private network link.

'705 Patent (Ex. 1050) at Claim 21



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

(10) **Patent**
(45) **Date o**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,958**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0117237 A1 May 10, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/1
(52) **U.S. Cl.**
USPC ......
(58) **Field of Cl**
USPC ......
See applica

(56)

U.S

2,895,502 A
4,677,434 A

FOREIGN PATENT DOCUMENTS

DE 19924575 12/1999

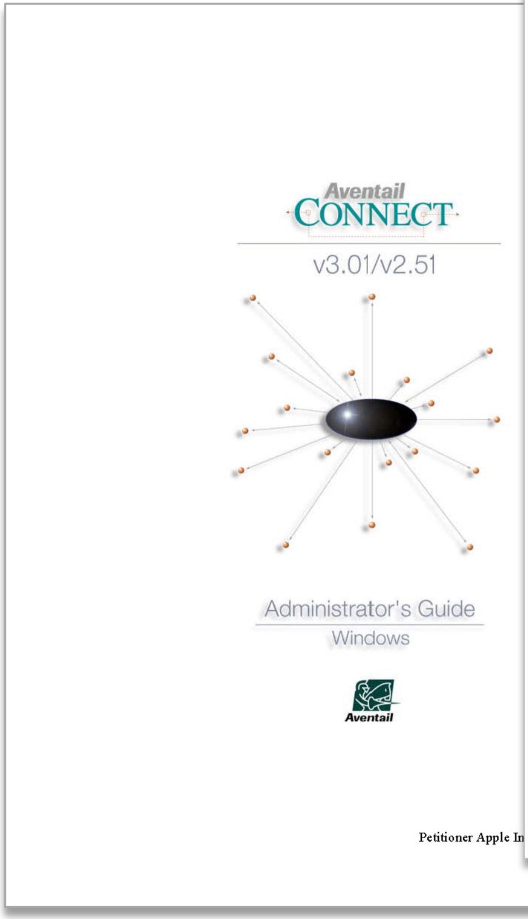
Secure Communication Link

Petitioner's Construction	**Patent Owner's Construction**
A transmission path that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping	A direct communication link that provides data security through encryption

Pet. (871) at 11-12; Resp. (871) at 5

Grounds Based on Aventail and RFCs 2401 & 2543

"[Direct] secure communications link"



Aventail CONNECT

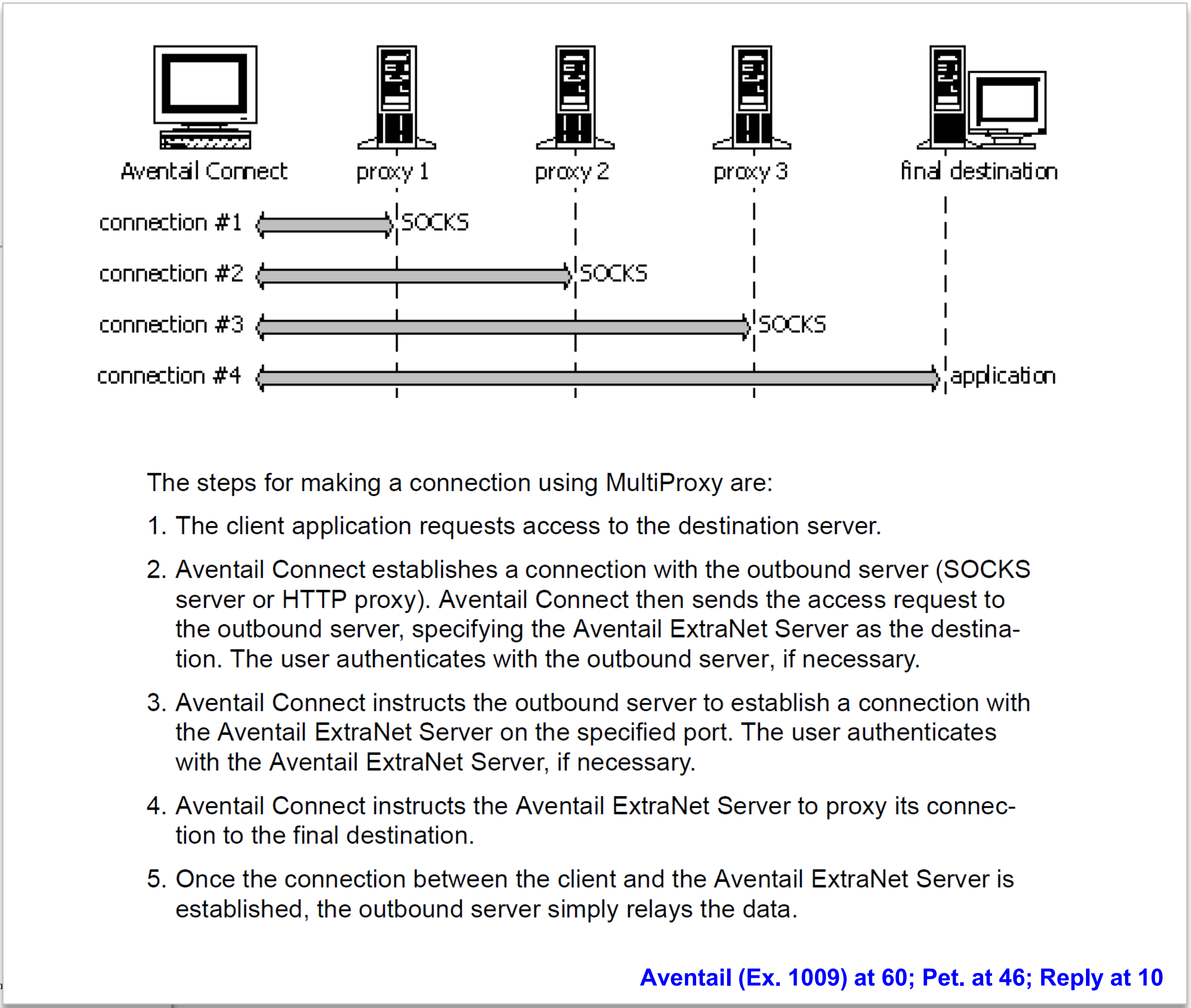
v3.01/v2.51

Administrator's Guide

Windows

Aventail

Petitioner Apple In



Aventail Connect
proxy 1
proxy 2
proxy 3
final destination
connection #1
SOCKS
connection #2
SOCKS
connection #3
SOCKS
connection #4
application

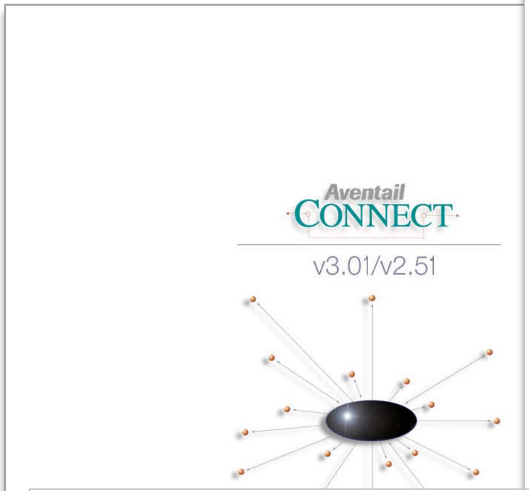
The steps for making a connection using MultiProxy are:

1. The client application requests access to the destination server.
2. Aventail Connect establishes a connection with the outbound server (SOCKS server or HTTP proxy). Aventail Connect then sends the access request to the outbound server, specifying the Aventail ExtraNet Server as the destination. The user authenticates with the outbound server, if necessary.
3. Aventail Connect instructs the outbound server to establish a connection with the Aventail ExtraNet Server on the specified port. The user authenticates with the Aventail ExtraNet Server, if necessary.
4. Aventail Connect instructs the Aventail ExtraNet Server to proxy its connection to the final destination.
5. Once the connection between the client and the Aventail ExtraNet Server is established, the outbound server simply relays the data.

Aventail (Ex. 1009) at 60; Pet. at 46; Reply at 10

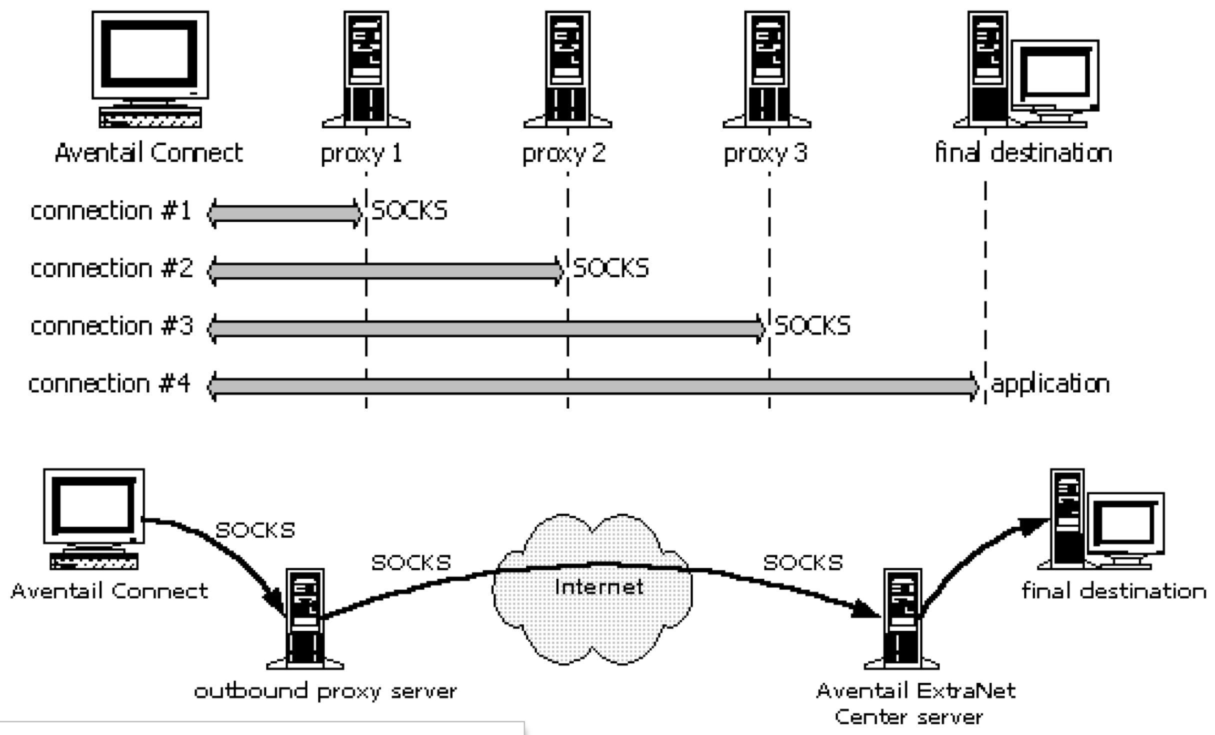
Grounds Based on Aventail and RFCs 2401 & 2543

"[Direct] secure communications link"

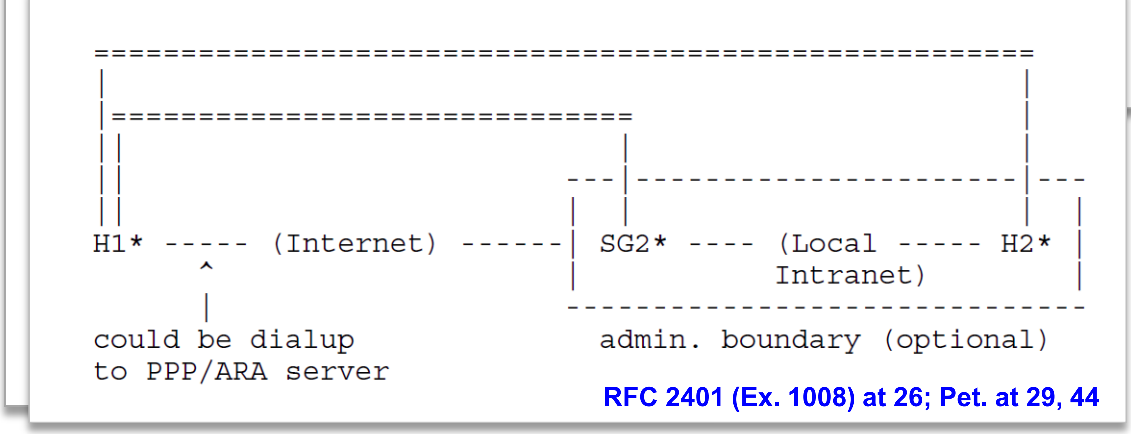


Aventail CONNECT

v3.01/v2.51



Aventail (Ex. 1009) at 60; Pet. at 46; Reply at 10

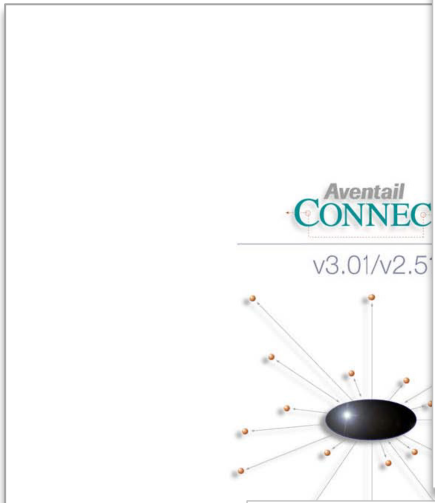


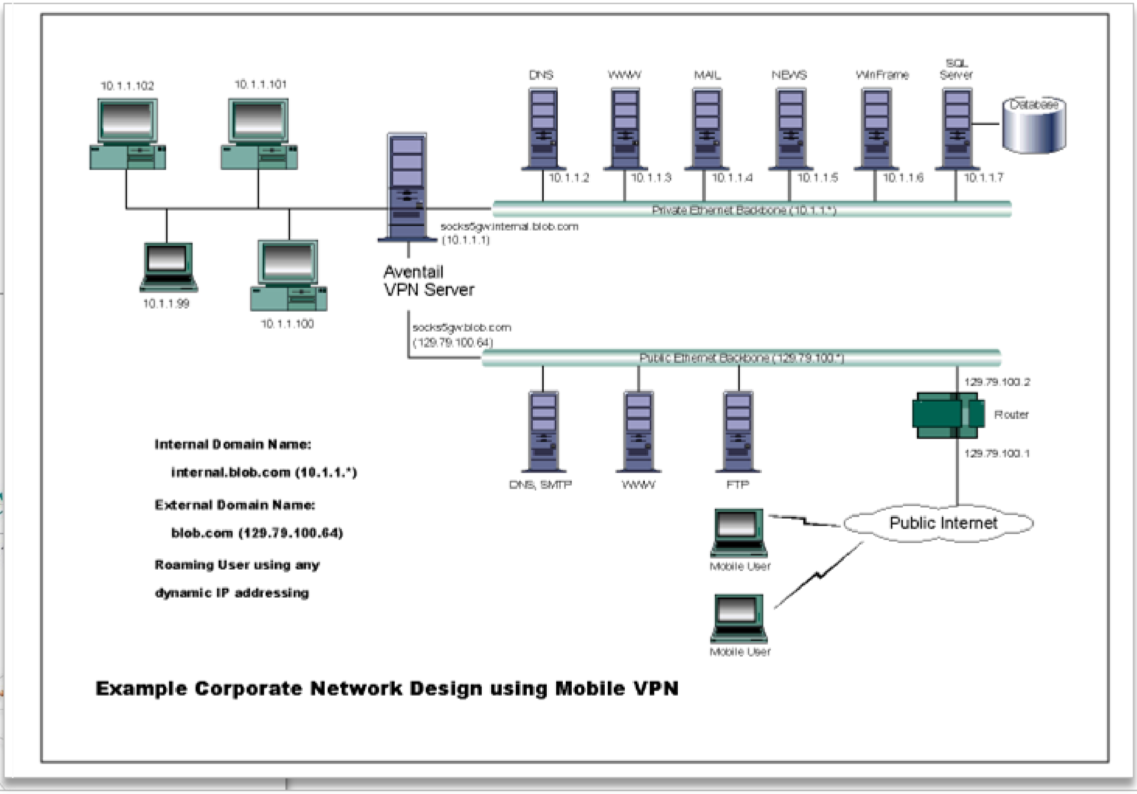
```
======================================================
|                                                    |
|==============================                      |
||                            |                      |
||                            |                      |
||                         ---|----------------------|---
||                         |  |                      |  |
H1* ----- (Internet) ------| SG2* ---- (Local ----- H2* |
      ^                    |           Intranet)        |
      |                    ------------------------------
could be dialup              admin. boundary (optional)
to PPP/ARA server
```

RFC 2401 (Ex. 1008) at 26; Pet. at 29, 44

Grounds Based on Aventail and RFCs 2401 & 2543

"[Direct] secure communications link"



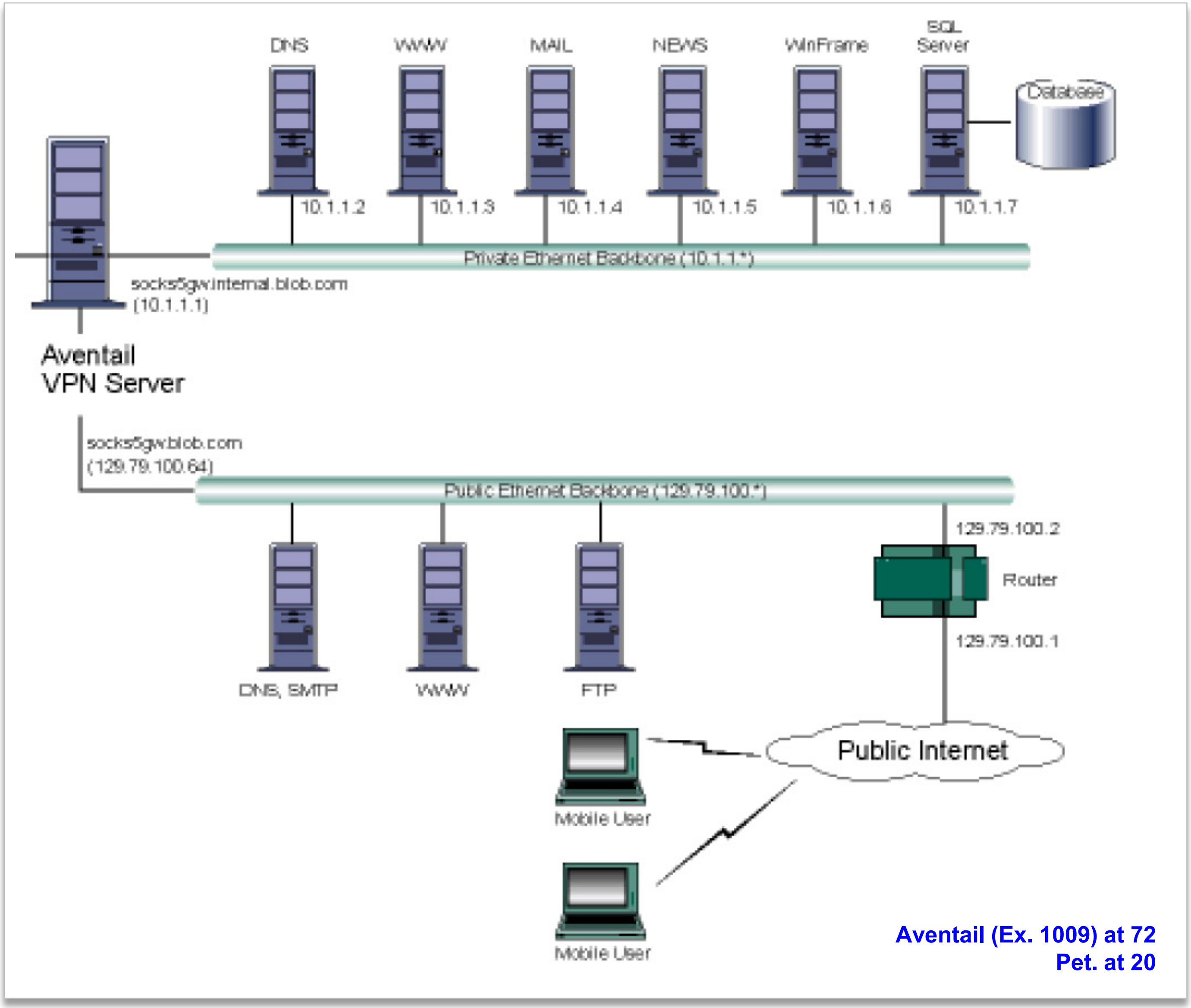


Example Corporate Network Design using Mobile VPN

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.

Aventail (Ex. 1009) at 72; Pet. (871) at 35, 44-45

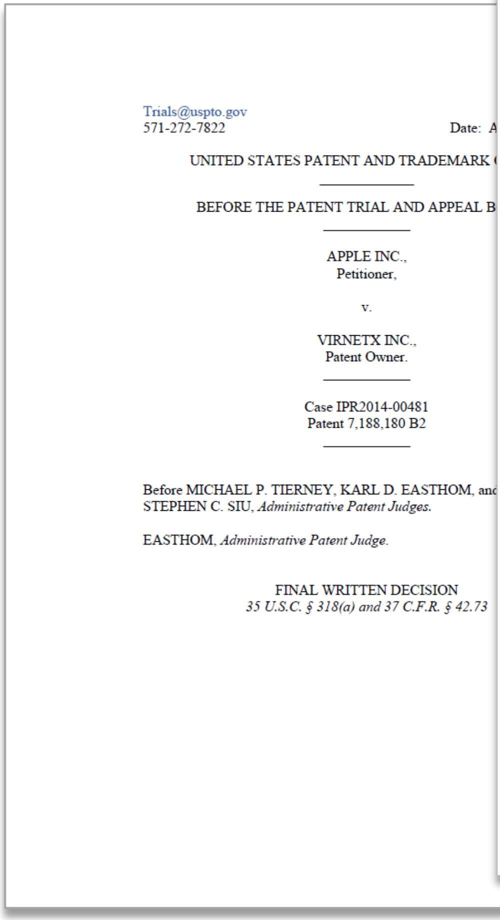
Grounds Based on Aventail and RFCs 2401 & 2543



Aventail (Ex. 1009) at 72
Pet. at 20

Final Written Decision in IPR2014-00481

"secure communication link" & "VPN link"



Trials@uspto.gov
571-272-7822

Date: A

UNITED STATES PATENT AND TRADEMARK

BEFORE THE PATENT TRIAL AND APPEAL B

APPLE INC.,
Petitioner,

v.

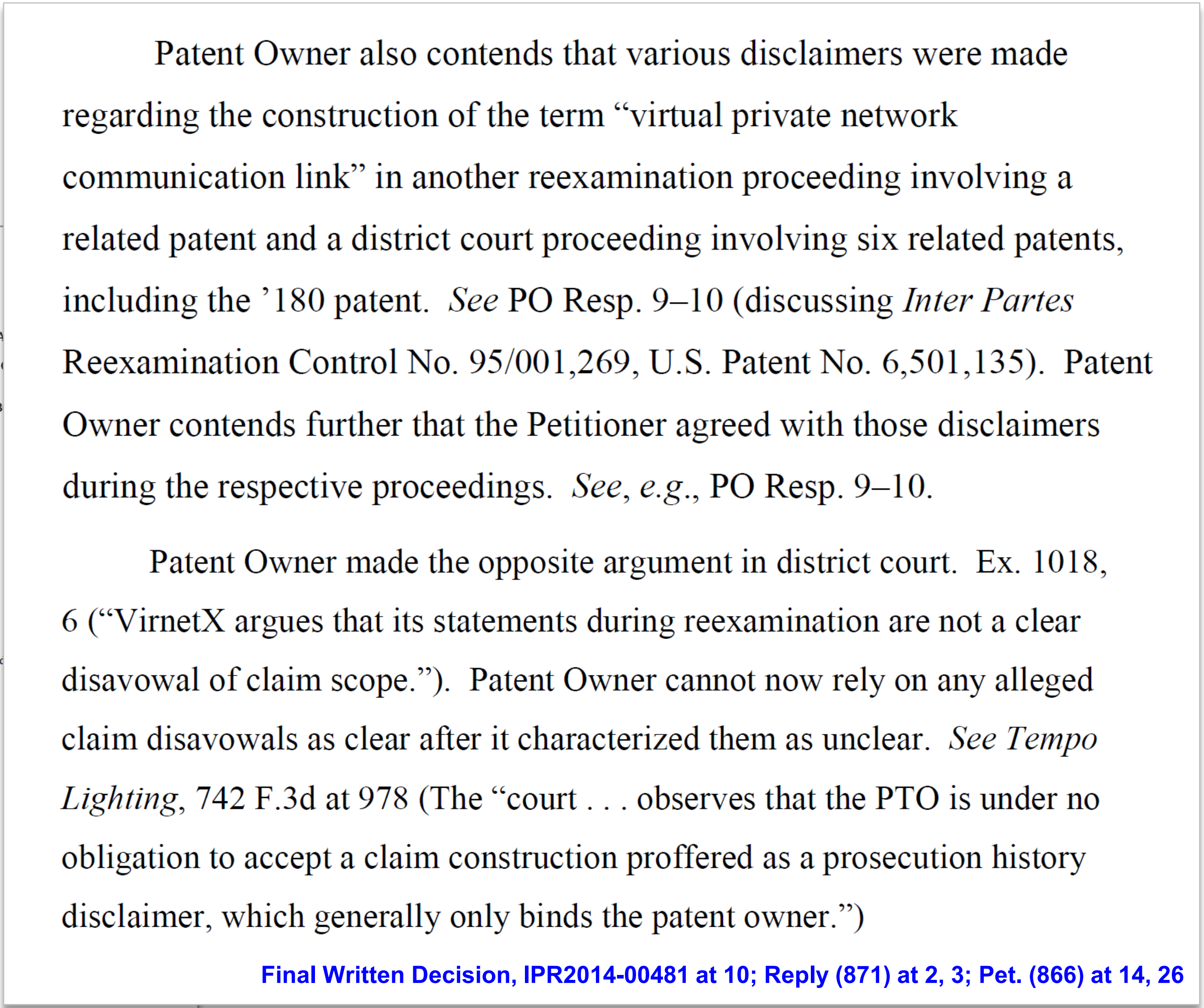
VIRNETX INC.,
Patent Owner.

Case IPR2014-00481
Patent 7,188,180 B2

Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and
STEPHEN C. SIU, *Administrative Patent Judges.*

EASTHOM, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

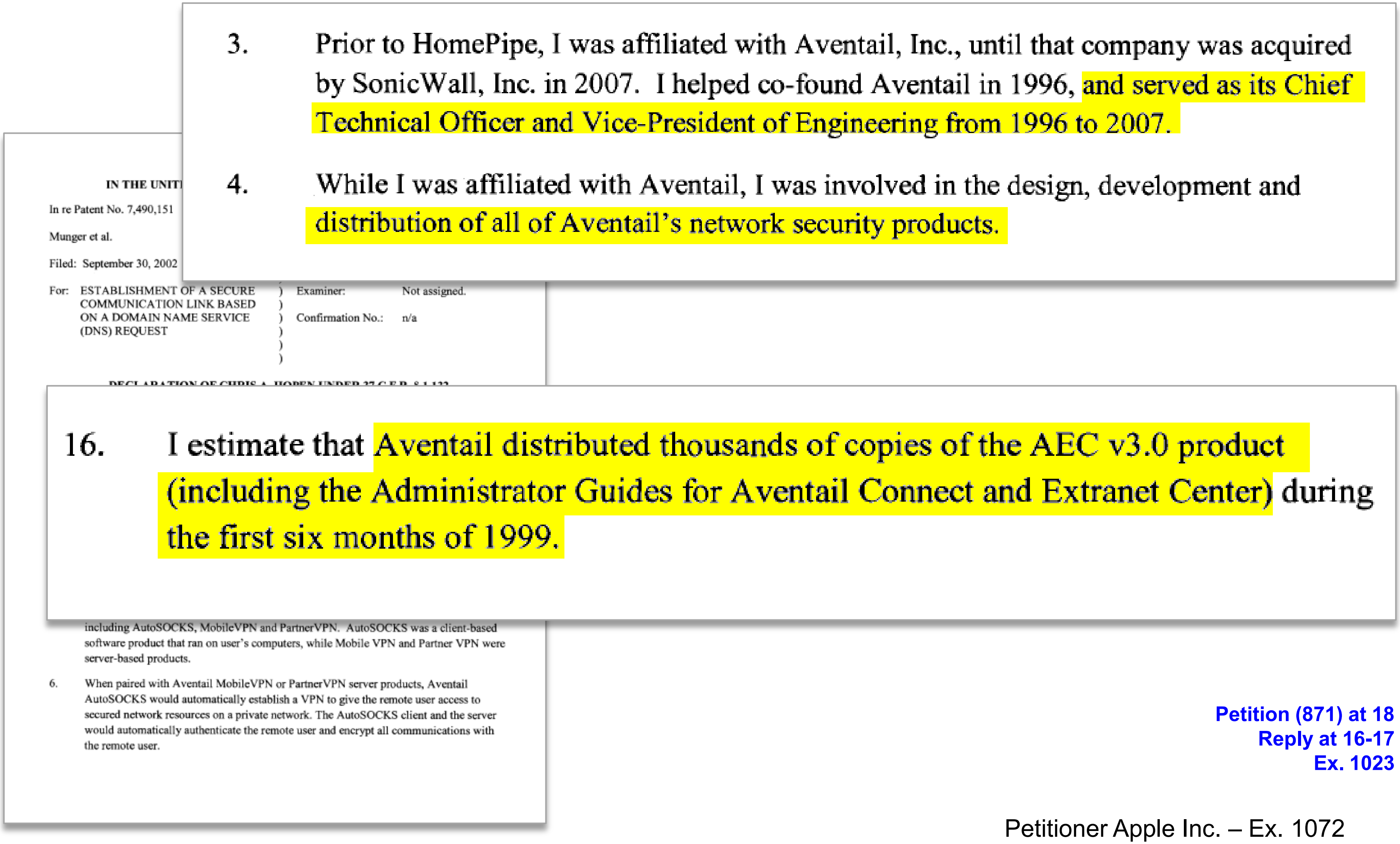


Patent Owner also contends that various disclaimers were made regarding the construction of the term "virtual private network communication link" in another reexamination proceeding involving a related patent and a district court proceeding involving six related patents, including the '180 patent. *See* PO Resp. 9–10 (discussing *Inter Partes* Reexamination Control No. 95/001,269, U.S. Patent No. 6,501,135). Patent Owner contends further that the Petitioner agreed with those disclaimers during the respective proceedings. *See, e.g.*, PO Resp. 9–10.

Patent Owner made the opposite argument in district court. Ex. 1018, 6 ("VirnetX argues that its statements during reexamination are not a clear disavowal of claim scope."). Patent Owner cannot now rely on any alleged claim disavowals as clear after it characterized them as unclear. *See Tempo Lighting*, 742 F.3d at 978 (The "court . . . observes that the PTO is under no obligation to accept a claim construction proffered as a prosecution history disclaimer, which generally only binds the patent owner.")

Final Written Decision, IPR2014-00481 at 10; Reply (871) at 2, 3; Pet. (866) at 14, 26

Declaration of Christopher A. Hopen



IN THE UNIT

In re Patent No. 7,490,151

Munger et al.

Filed: September 30, 2002

For: ESTABLISHMENT OF A SECURE COMMUNICATION LINK BASED ON A DOMAIN NAME SERVICE (DNS) REQUEST) Examiner: Not assigned.

) Confirmation No.: n/a

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

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.

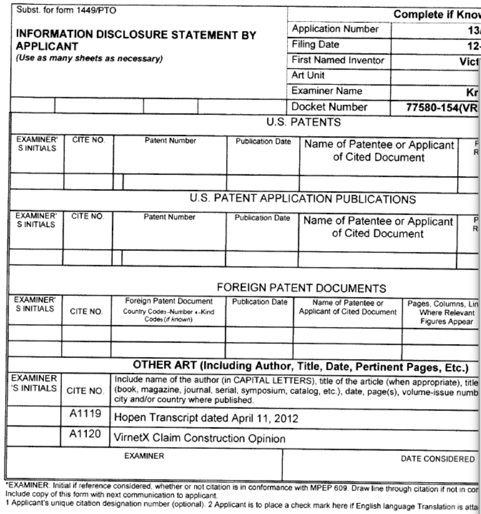
16. I estimate that Aventail distributed thousands of copies of the AEC v3.0 product (including the Administrator Guides for Aventail Connect and Extranet Center) during the first six months of 1999.

including AutoSOCKS, MobileVPN and PartnerVPN. AutoSOCKS was a client-based software product that ran on user's computers, while Mobile VPN and Partner VPN were server-based products.

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 (871) at 18
Reply at 16-17
Ex. 1023

Cross-Examination of Christopher A. Hopen



Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	13/339,257
Filing Date	12-28-2011
First Named Inventor	Vict
Art Unit	
Examiner Name	Kr
Docket Number	77580-154(VR

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	P R

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	P R

FOREIGN PATENT DOCUMENTS

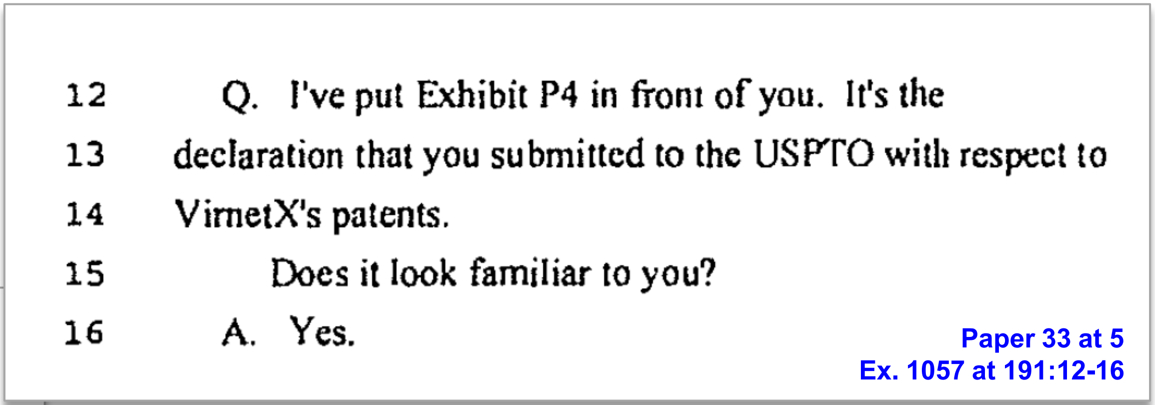
EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 -Number 4 -Kind Codes (if known)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lin Where Relevant Figures Appear

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue numb city and/or country where published.
	A1119	Hopen Transcript dated April 11, 2012
	A1120	VirnetX Claim Construction Opinion

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in cor
Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is atta

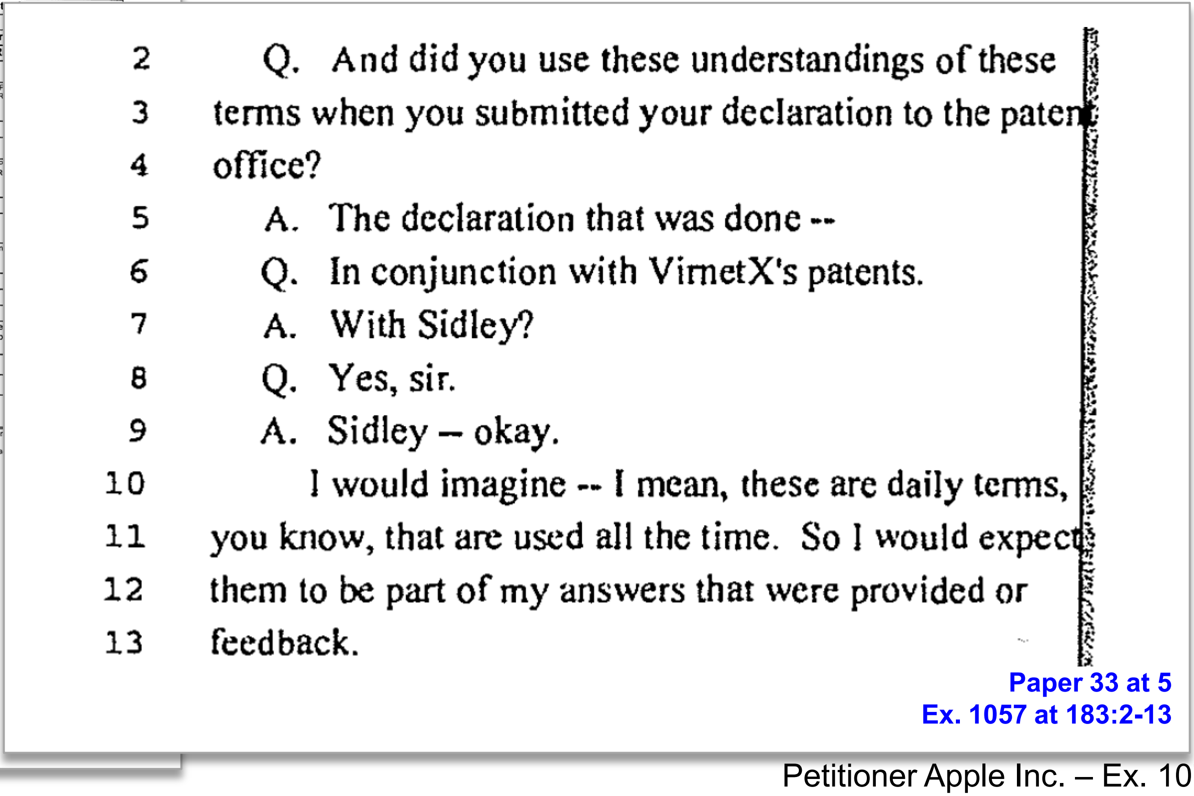


Q. I've put Exhibit P4 in front of you. It's the declaration that you submitted to the USPTO with respect to VirnetX's patents.

Does it look familiar to you?

A. Yes.

Paper 33 at 5
Ex. 1057 at 191:12-16



Q. And did you use these understandings of these terms when you submitted your declaration to the patent office?

A. The declaration that was done --

Q. In conjunction with VirnetX's patents.

A. With Sidley?

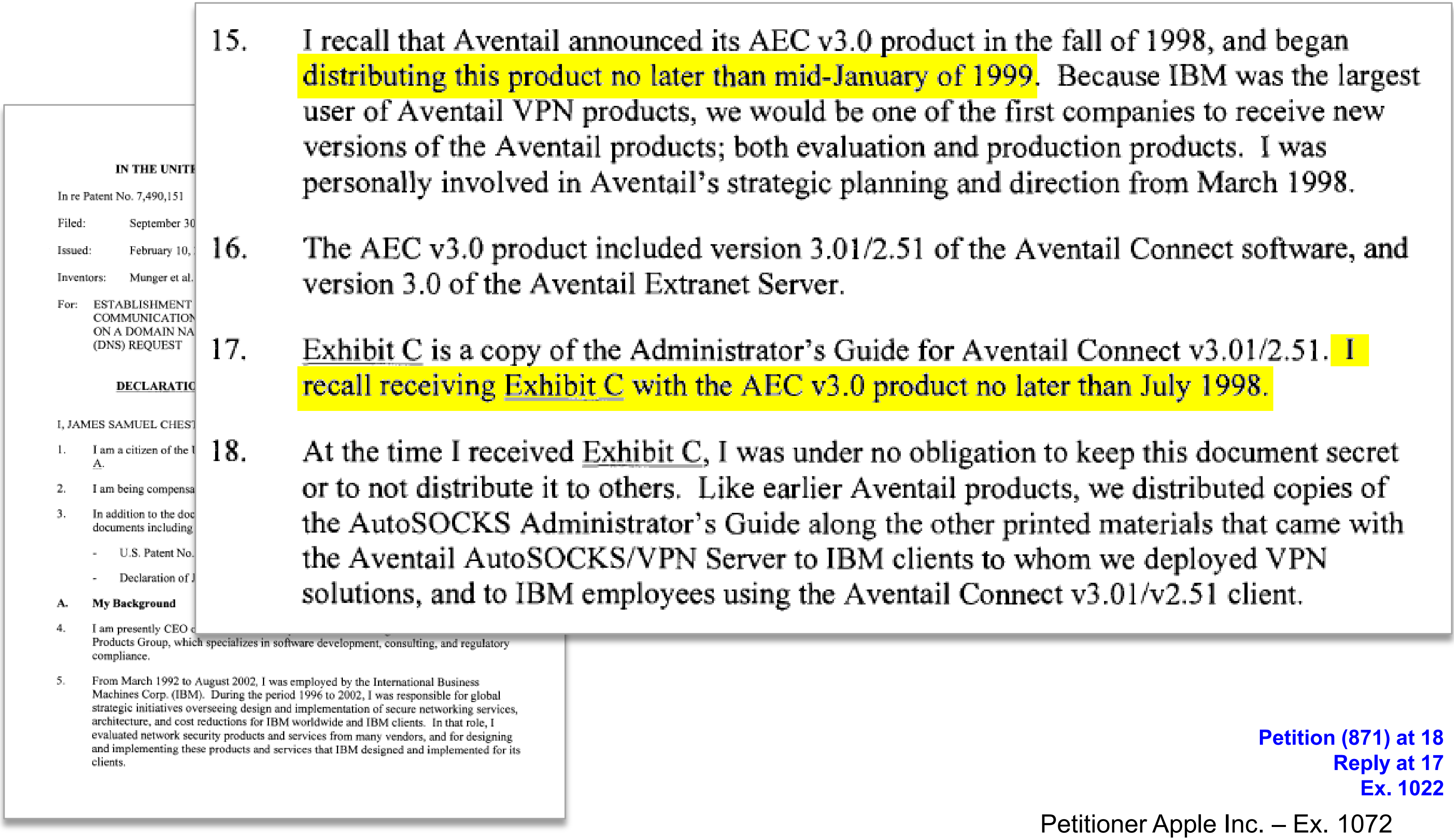
Q. Yes, sir.

A. Sidley -- okay.

I would imagine -- I mean, these are daily terms, you know, that are used all the time. So I would expect them to be part of my answers that were provided or feedback.

Paper 33 at 5
Ex. 1057 at 183:2-13

Declaration of James Chester



IN THE UNITE

In re Patent No. 7,490,151

Filed: September 30

Issued: February 10,

Inventors: Munger et al.

For: ESTABLISHMENT
COMMUNICATION
ON A DOMAIN NA
(DNS) REQUEST

DECLARATIO

I, JAMES SAMUEL CHEST

1. I am a citizen of the U
A.

2. I am being compensa

3. In addition to the doc
documents including

- U.S. Patent No.
- Declaration of J

A. **My Background**

4. I am presently CEO o
Products Group, which specializes in software development, consulting, and regulatory compliance.

5. From March 1992 to August 2002, I was employed by the International Business Machines Corp. (IBM). During the period 1996 to 2002, I was responsible for global 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.

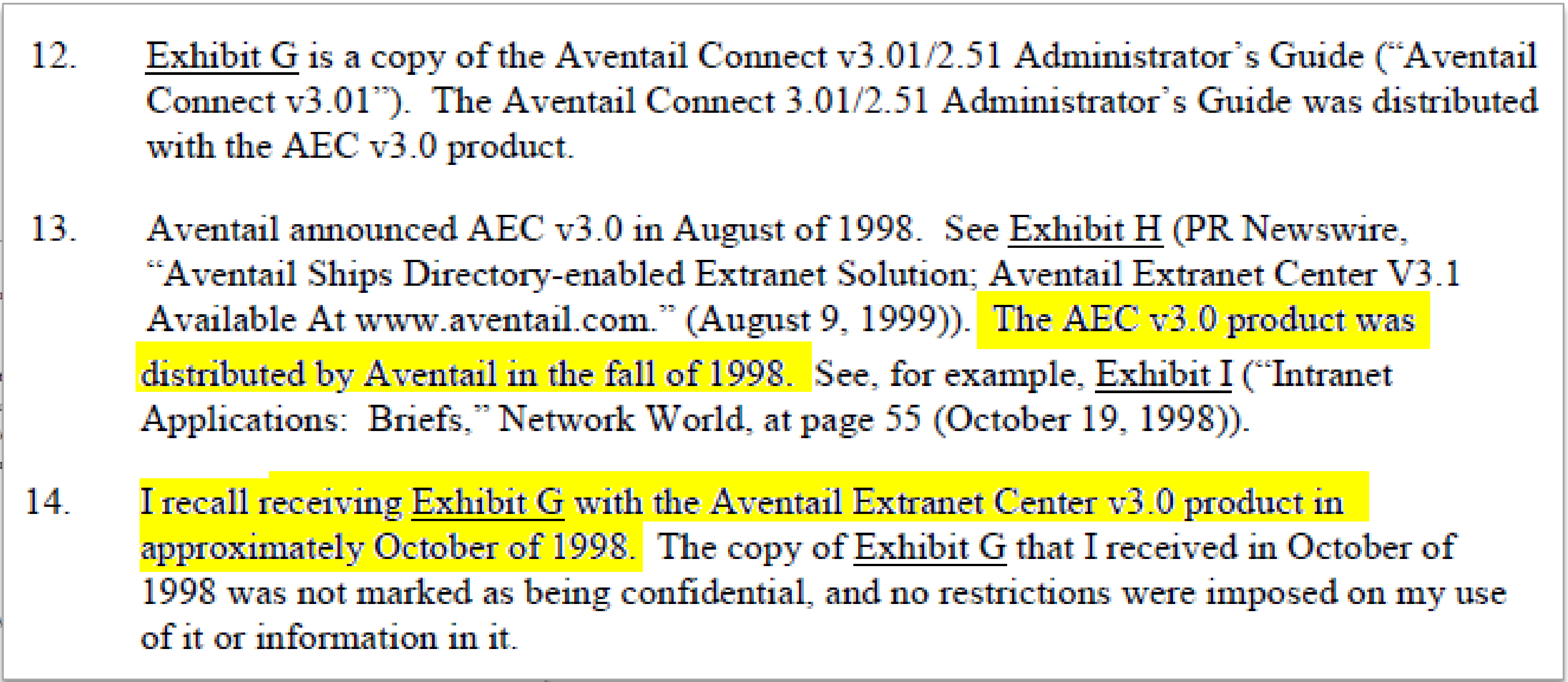
16. The AEC v3.0 product included version 3.01/2.51 of the Aventail Connect software, and version 3.0 of the Aventail Extranet Server.

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 (871) at 18
Reply at 17
Ex. 1022

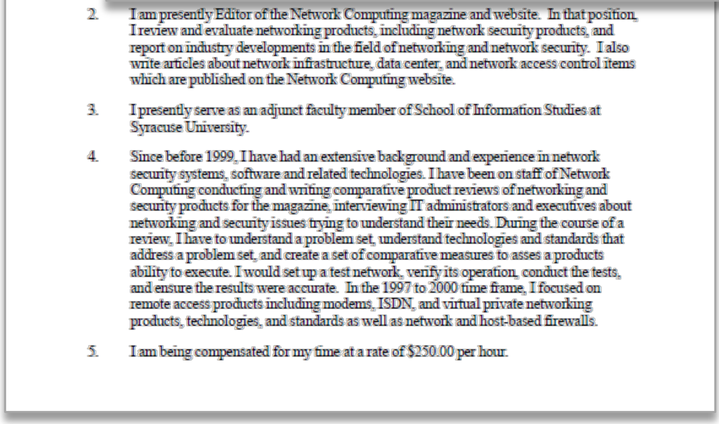
Declaration of Michael Allyn Fratto



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.



In r

Pat

Mu

File

For

I, M

1.

2. I am presently Editor of the Network Computing magazine and website. In that position, I review and evaluate networking products, including network security products, and report on industry developments in the field of networking and network security. I also write articles about network infrastructure, data center, and network access control items 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.

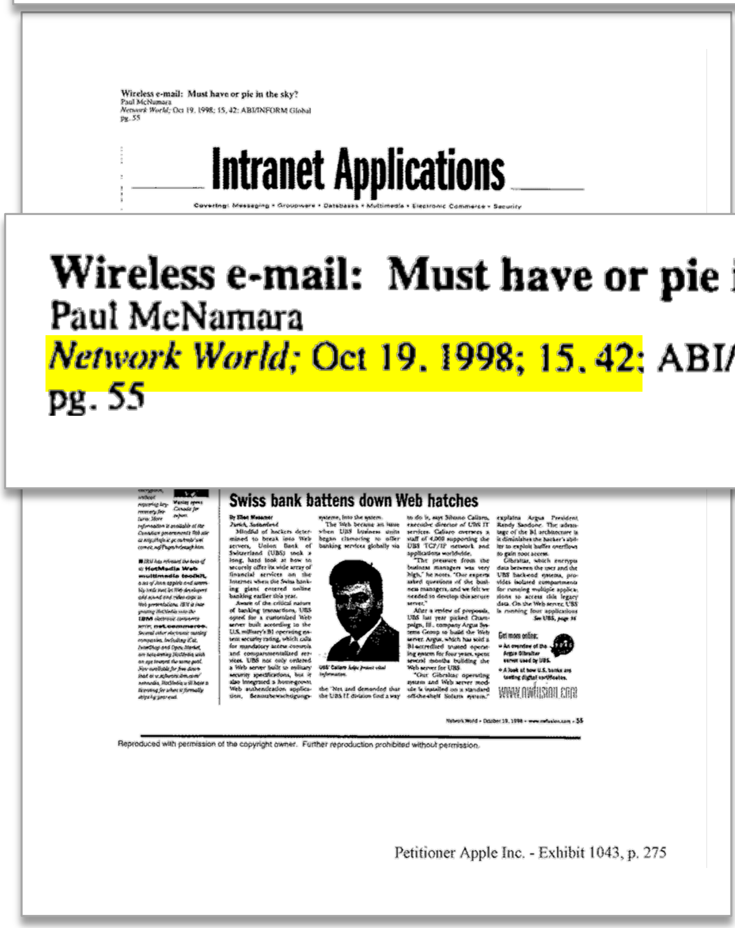
5. I am being compensated for my time at a rate of $250.00 per hour.

Petition (871) at 18
Reply at 17
Ex. 1043

Exhibit I to
Declaration of Michael Allyn Fratto

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)).

Ex. 1043 at ¶13; Paper 33 at 3



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

Intranet Applications

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

Swiss bank battens down Web hatches

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

Petitioner Apple Inc. - Exhibit 1043, p. 275

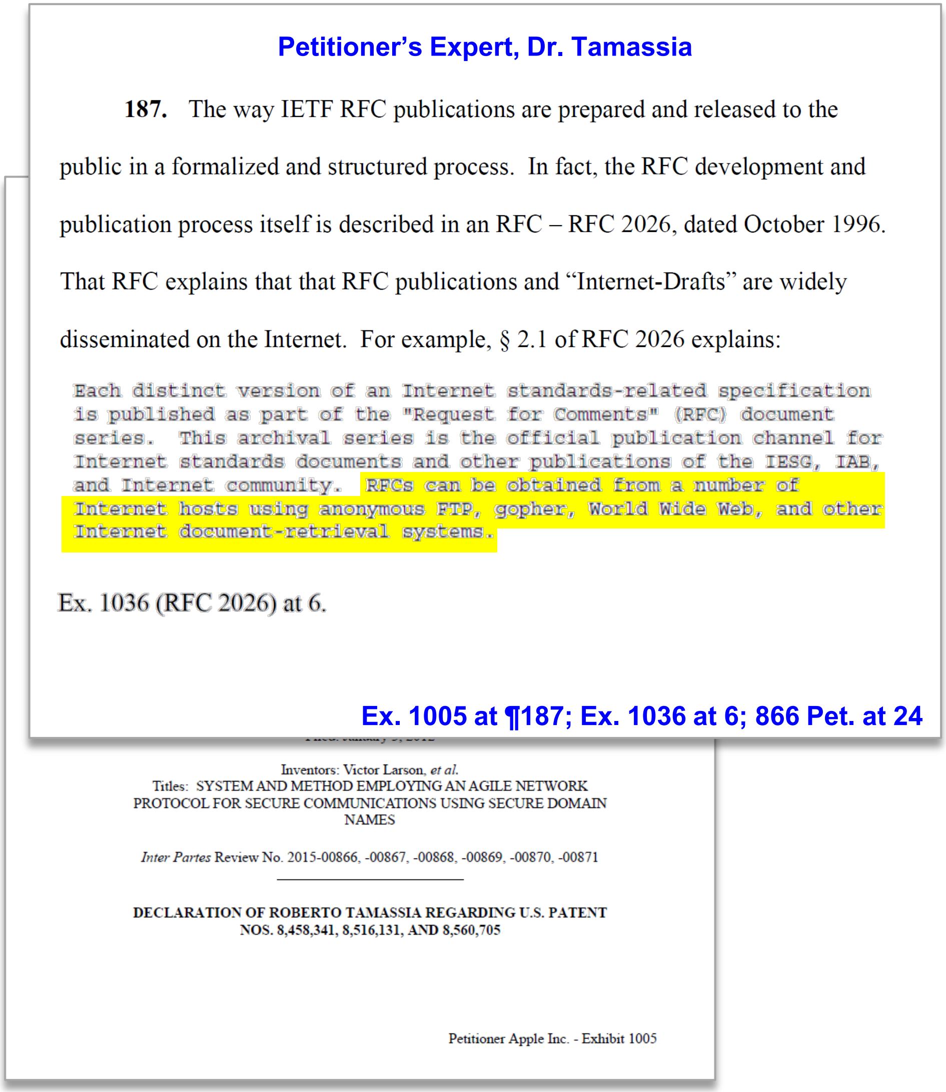
Wireless e-mail: Must have or pie in the sky?
Paul McNamara
Network World; Oct 19, 1998; 15, 42; ABI/INFORM Global
pg. 55

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 ExtraNet 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*

Ex. 1043 at 275

RFCs



Petitioner's Expert, Dr. Tamassia

187. 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 ¶187; Ex. 1036 at 6; 866 Pet. at 24

Filed: January 9, 2012

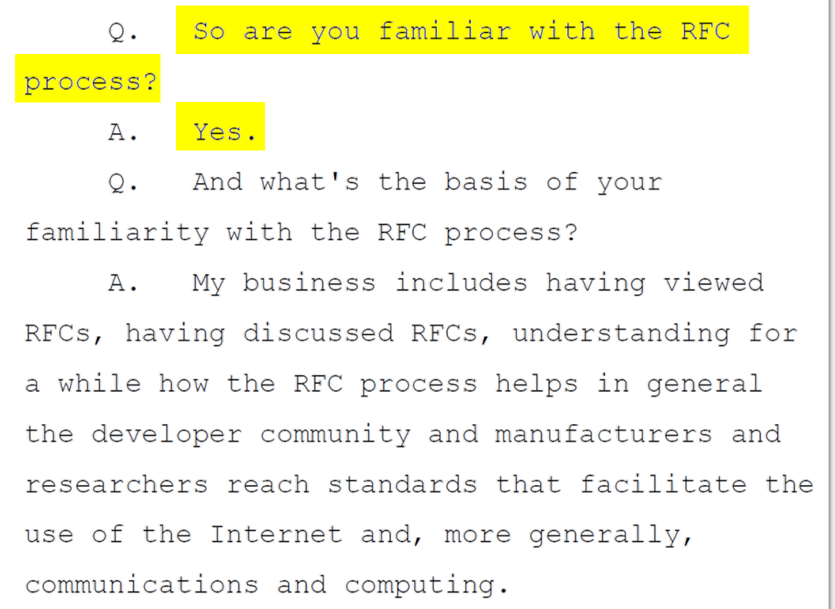
Inventors: Victor Larson, *et al.*
Titles: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Inter Partes Review No. 2015-00866, -00867, -00868, -00869, -00870, -00871

DECLARATION OF ROBERTO TAMASSIA REGARDING U.S. PATENT NOS. 8,458,341, 8,516,131, AND 8,560,705

Petitioner Apple Inc. - Exhibit 1005

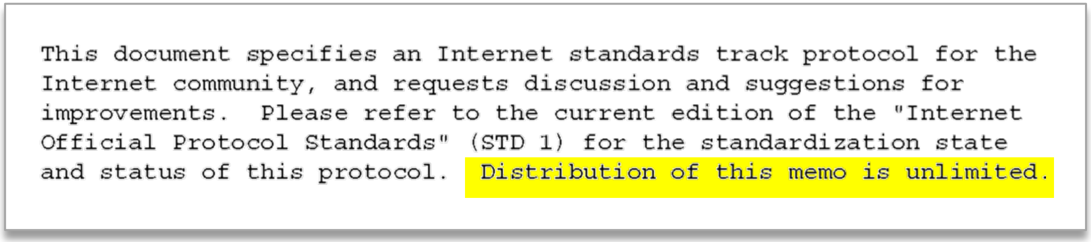
Petitioner's Expert, Dr. Tamassia



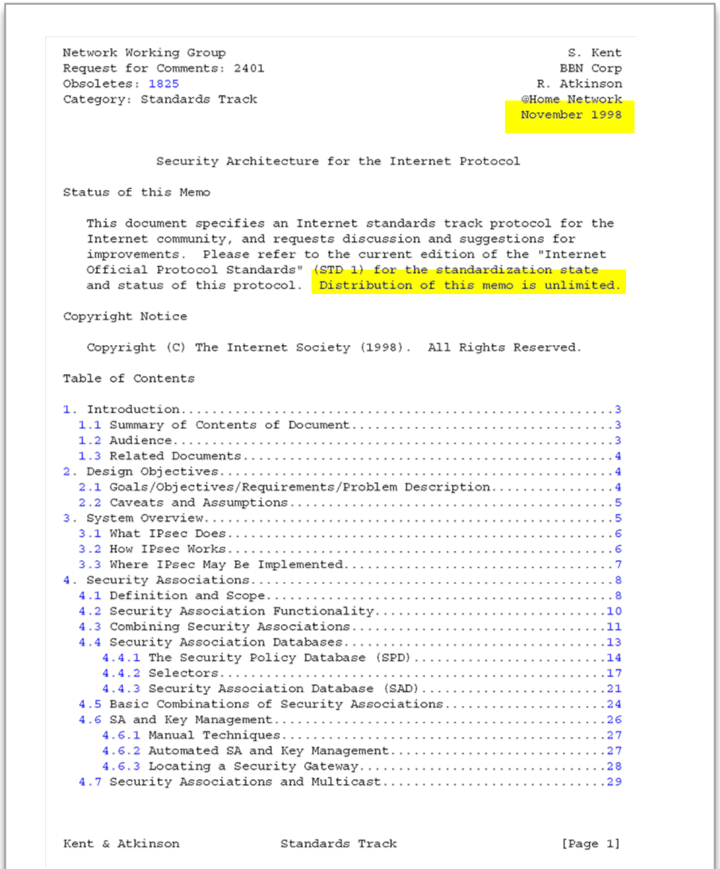
```
     Q.   So are you familiar with the RFC
process?
     A.   Yes.
     Q.   And what's the basis of your
familiarity with the RFC process?
     A.   My business includes having viewed
RFCs, having discussed RFCs, understanding for
a while how the RFC process helps in general
the developer community and manufacturers and
researchers reach standards that facilitate the
use of the Internet and, more generally,
communications and computing.
```

Ex. 2019 at 103:1-13; Reply (866) at 21

RFCs



This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

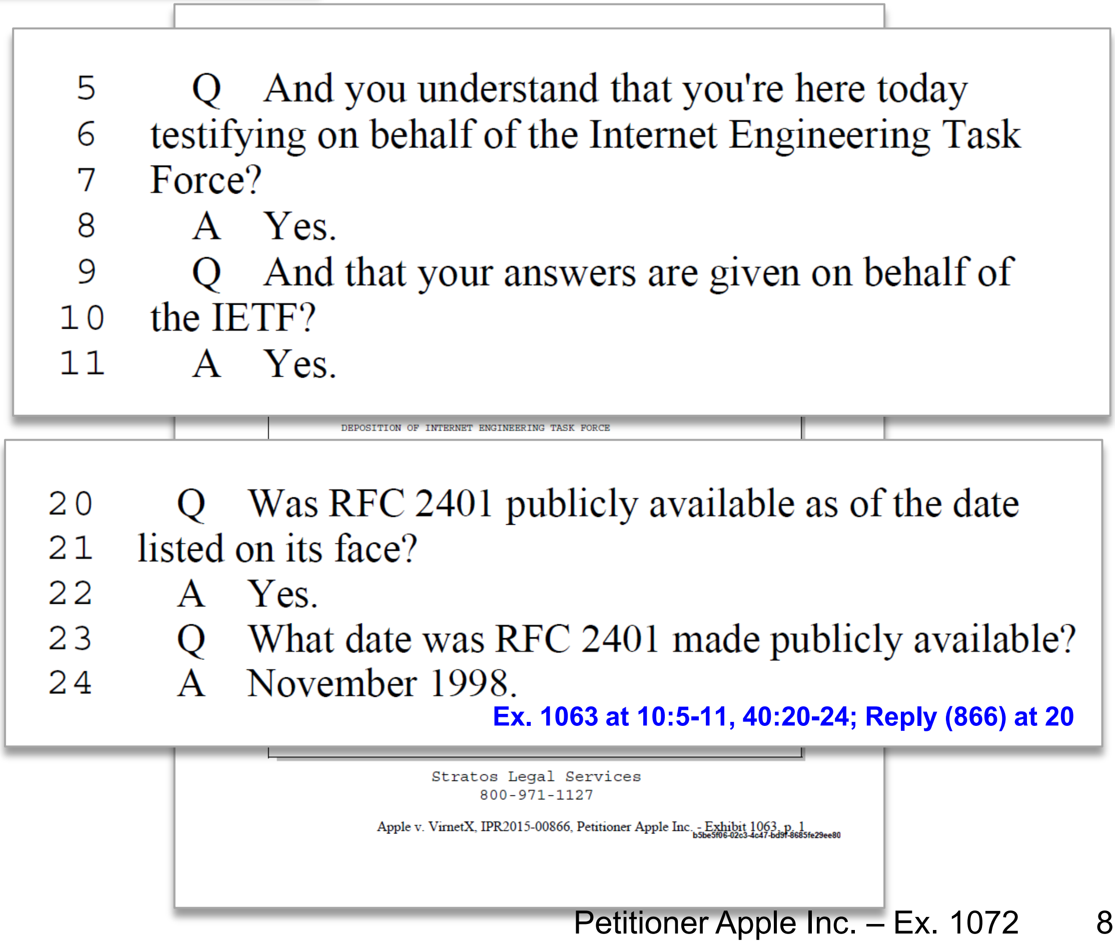


```
Network Working Group                                          S. Kent
Request for Comments: 2401                                    BBN Corp
Obsoletes: 1825                                            R. Atkinson
Category: Standards Track                                @Home Network
                                                         November 1998

              Security Architecture for the Internet Protocol

Status of this Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements.  Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol.  Distribution of this memo is unlimited.

Copyright Notice

   Copyright (C) The Internet Society (1998).  All Rights Reserved.

Table of Contents
```

```
1. Introduction........................................................3
  1.1 Summary of Contents of Document..................................3
  1.2 Audience.........................................................3
  1.3 Related Documents................................................4
2. Design Objectives...................................................4
  2.1 Goals/Objectives/Requirements/Problem Description................4
  2.2 Caveats and Assumptions..........................................5
3. System Overview.....................................................5
  3.1 What IPsec Does..................................................6
  3.2 How IPsec Works..................................................6
  3.3 Where IPsec May Be Implemented...................................7
4. Security Associations...............................................8
  4.1 Definition and Scope.............................................8
  4.2 Security Association Functionality..............................10
  4.3 Combining Security Associations.................................11
  4.4 Security Association Databases..................................13
     4.4.1 The Security Policy Database (SPD).........................14
     4.4.2 Selectors..................................................17
     4.4.3 Security Association Database (SAD)........................21
  4.5 Basic Combinations of Security Associations.....................24
  4.6 SA and Key Management...........................................26
     4.6.1 Manual Techniques..........................................27
     4.6.2 Automated SA and Key Management............................27
     4.6.3 Locating a Security Gateway................................28
  4.7 Security Associations and Multicast.............................29
```

```
Kent & Atkinson              Standards Track                    [Page 1]
```

Ex. 1008 at 1; 866 Pet. at 24



Q And you understand that you're here today testifying on behalf of the Internet Engineering Task Force?

A Yes.

Q And that your answers are given on behalf of the IETF?

A Yes.

DEPOSITION OF INTERNET ENGINEERING TASK FORCE

Q Was RFC 2401 publicly available as of the date listed on its face?

A Yes.

Q What date was RFC 2401 made publicly available?

A November 1998.

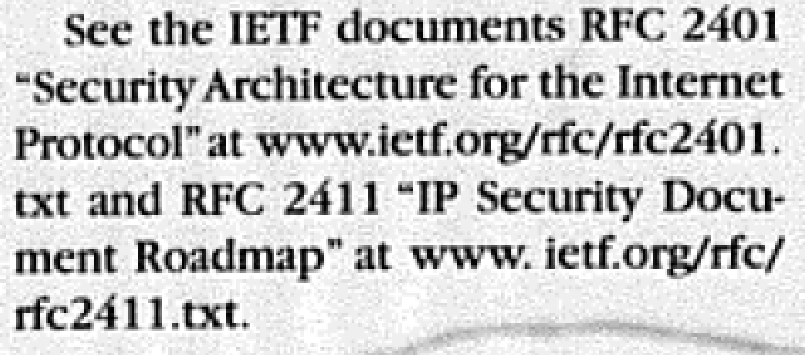
Ex. 1063 at 10:5-11, 40:20-24; Reply (866) at 20

Stratos Legal Services
800-971-1127

Apple v. VirnetX, IPR2015-00866, Petitioner Apple Inc. - Exhibit 1063, p. 1
b5be5f06-02c3-4c47-bd9f-8685fe29ee80

RFCs

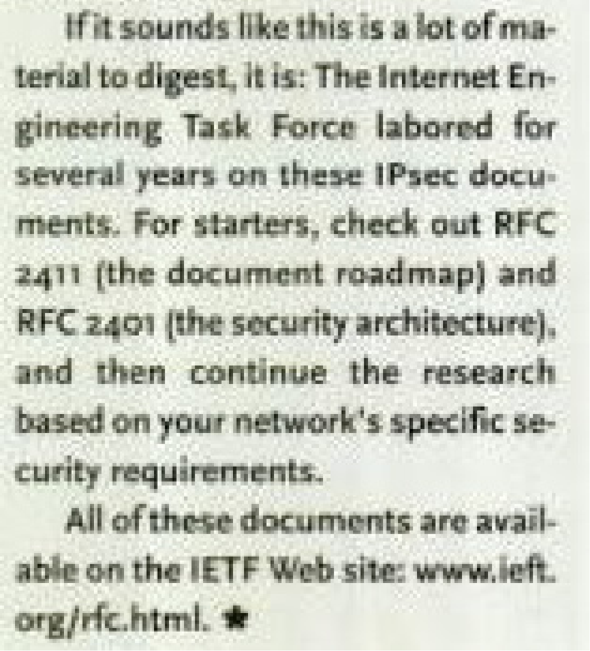
NetworkWorld, Mar. 15, 1999



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; 866 Reply at 20

InfoWorld, Aug. 16, 1999



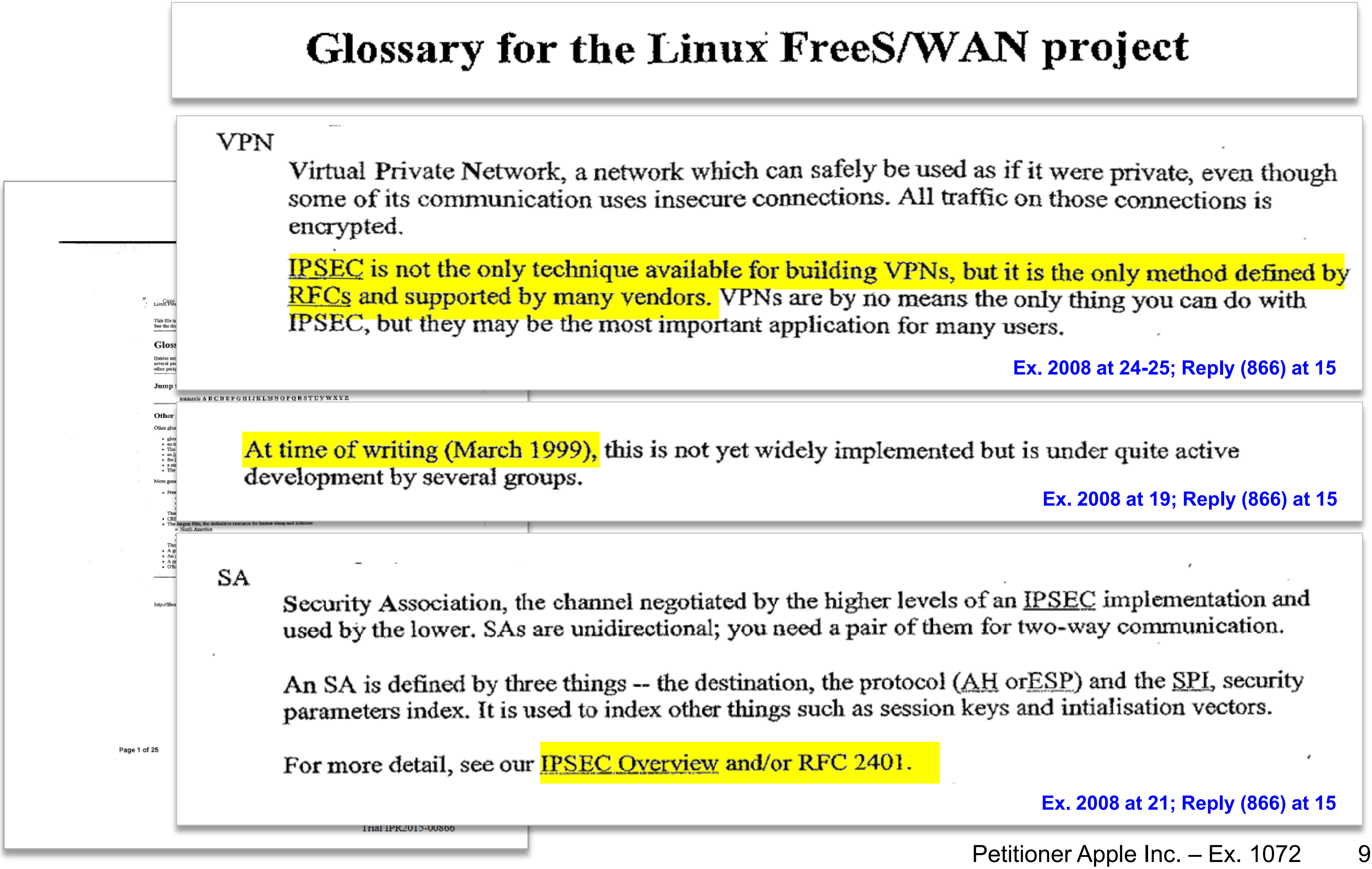
If it sounds like this is a lot of material to digest, it is: The Internet Engineering Task Force labored for several years on these IPsec documents. For starters, check out RFC 2411 (the document roadmap) and RFC 2401 (the security architecture), and then continue the research based on your network's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

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

Ex. 1064 at 9; 866 Reply at 20

Patent Owner Admission

RFC 2401



Glossary for the Linux FreeS/WAN project

VPN

Virtual Private Network, a network which can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted.

IPSEC is not the only technique available for building VPNs, but it is the only method defined by RFCs and supported by many vendors. VPNs are by no means the only thing you can do with IPSEC, but they may be the most important application for many users.

Ex. 2008 at 24-25; Reply (866) at 15

At time of writing (March 1999), this is not yet widely implemented but is under quite active development by several groups.

Ex. 2008 at 19; Reply (866) at 15

SA

Security Association, the channel negotiated by the higher levels of an IPSEC implementation and used by the lower. SAs are unidirectional; you need a pair of them for two-way communication.

An SA is defined by three things -- the destination, the protocol (AH orESP) and the SPI, security parameters index. It is used to index other things such as session keys and intialisation vectors.

For more detail, see our IPSEC Overview and/or RFC 2401.

Ex. 2008 at 21; Reply (866) at 15

numeric A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

The Jargon File, the definitive resource for hacker slang and folklore

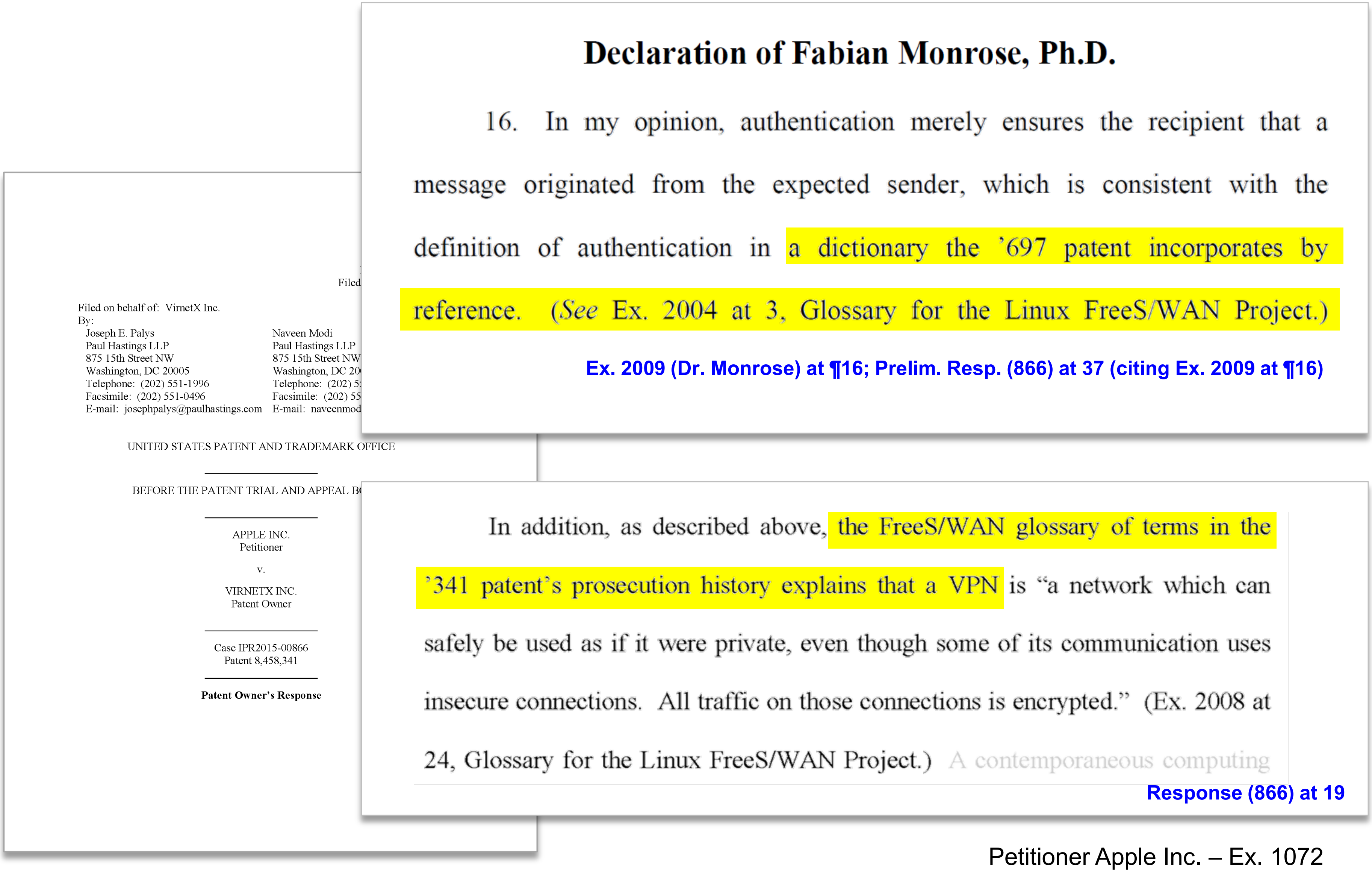
North America

Page 1 of 25

Trial IPR2015-00866

Patent Owner Admission

RFC 2401



Declaration of Fabian Monrose, Ph.D.

16. In my opinion, authentication merely ensures the recipient that a message originated from the expected sender, which is consistent with the definition of authentication in a dictionary the ’697 patent incorporates by reference. (*See* Ex. 2004 at 3, Glossary for the Linux FreeS/WAN Project.)

Ex. 2009 (Dr. Monrose) at ¶16; Prelim. Resp. (866) at 37 (citing Ex. 2009 at ¶16)

In addition, as described above, the FreeS/WAN glossary of terms in the ’341 patent’s prosecution history explains that a VPN is “a network which can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted.” (Ex. 2008 at 24, Glossary for the Linux FreeS/WAN Project.) A contemporaneous computing

Response (866) at 19

Filed

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 Modi
Paul Hastings LLP
875 15th Street NW
Washington, DC 20
Telephone: (202) 5
Facsimile: (202) 55
E-mail: naveenmod

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL B

APPLE INC.
Petitioner

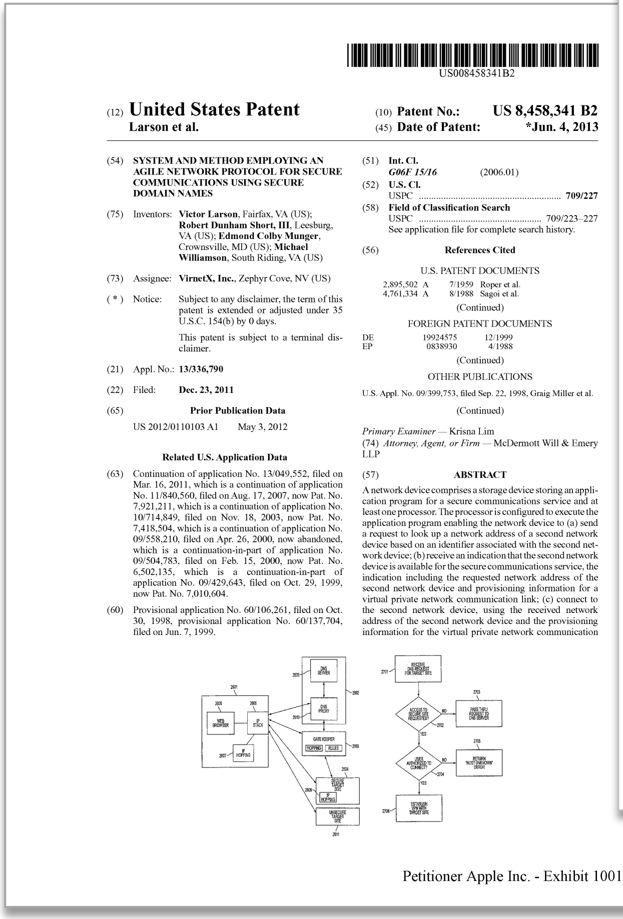
v.

VIRNETX INC.
Patent Owner

Case IPR2015-00866
Patent 8,458,341

Patent Owner’s Response

’341 Patent, Claim 1



US008458341B2

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

(10) **Patent No.:** **US 8,458,341 B2**
(45) **Date of Patent:** ***Jun. 4, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,790**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0110103 A1 May 3, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,761,334	A	8/1988	Sagoi et al.

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

U.S. Appl. No. 09/399,753, filed Sep. 22, 1998, Graig Miller et al.

(Continued)

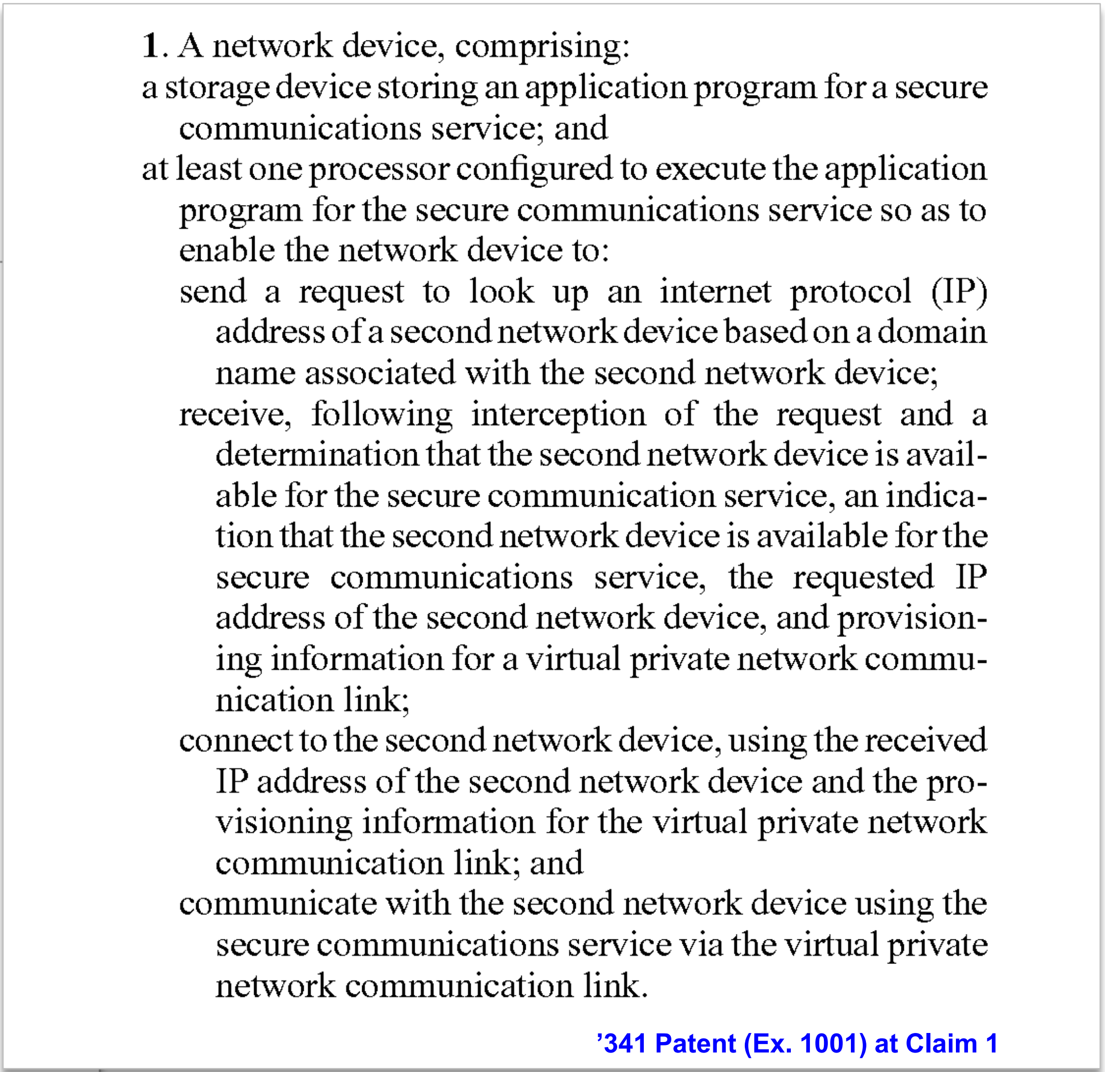
Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

A network device comprises a storage device storing an application program for a secure communications service and at least one processor. The processor is configured to execute the application program enabling the network device to (a) send a request to look up a network address of a second network device based on an identifier associated with the second network device; (b) receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link; (c) connect to the second network device, using the received network address of the second network device and the provisioning information for the virtual private network communication

RECEIVE DNS REQUEST FOR TARGET SITE
ACCESS TO SECURE SITE REQUESTED?
PASS THRU REQUEST TO DNS SERVER
NO
YES
DNS SERVER
DNS PROXY
GATE KEEPER
WEB BROWSER
IP STACK
IP HOPPING
HOPPING
RULES
SECURE TARGET SITE
UNSECURE TARGET SITE
USER AUTHORIZED TO CONNECT?
RETURN "HOST UNKNOWN" ERROR
ESTABLISH VPN WITH TARGET SITE
2601
2602
2609
2610
2605
2606
2701
2703

Petitioner Apple Inc. - Exhibit 1001, p. 1



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 request to look up an internet protocol (IP) address of a second network device based on a domain name associated with the second network device;

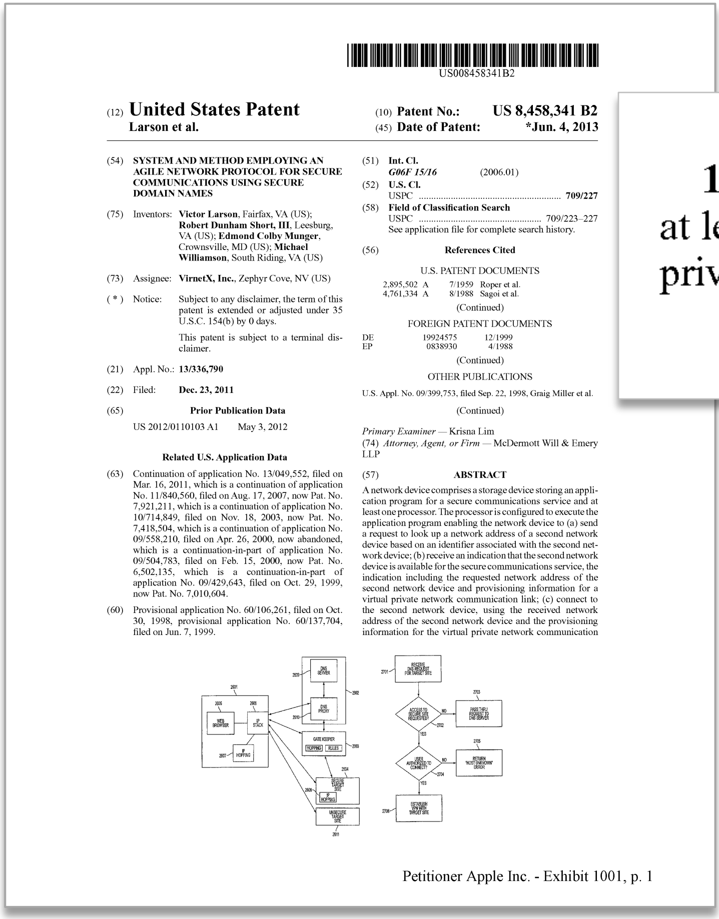
receive, following interception of the request and a determination that the second network device is available for the secure communication service, an indication that the second network device is available for the secure communications service, the requested IP address of the second network device, and provisioning information for a virtual private network communication link;

connect to the second network device, using the received IP address of the second network device and the provisioning information for the virtual private network communication link; and

communicate with the second network device using the secure communications service via the virtual private network communication link.

’341 Patent (Ex. 1001) at Claim 1

’341 Patent, Claim 17



US008458341B2

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

(10) **Patent No.: US 8,458,341 B2**
(45) **Date of Patent: *Jun. 4, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,790**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0110103 A1 May 3, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,761,334	A	8/1988	Sagoi et al.

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

U.S. Appl. No. 09/399,753, filed Sep. 22, 1998, Graig Miller et al.

(Continued)

Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

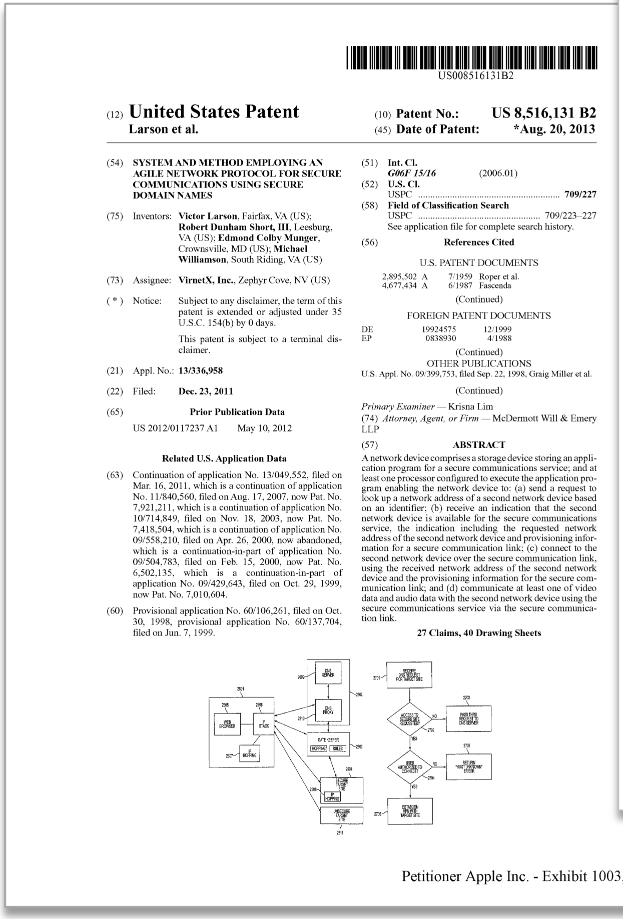
A network device comprises a storage device storing an application program for a secure communications service and at least one processor. The processor is configured to execute the application program enabling the network device to (a) send a request to look up a network address of a second network device based on an identifier associated with the second network device; (b) receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link; (c) connect to the second network device, using the received network address of the second network device and the provisioning information for the virtual private network communication

Petitioner Apple Inc. - Exhibit 1001, p. 1

17. The method of claim **15**, further comprising encrypting at least one of the video data and audio data over the virtual private network communication link.

’341 Patent (Ex. 1001) at Claim 17

’131 Patent, Claim 1



US008516131B2

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

(10) **Patent No.:** **US 8,516,131 B2**
(45) **Date of Patent:** ***Aug. 20, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,958**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0117237 A1 May 10, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,677,434	A	6/1987	Fascenda

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

U.S. Appl. No. 09/399,753, filed Sep. 22, 1998, Graig Miller et al.

(Continued)

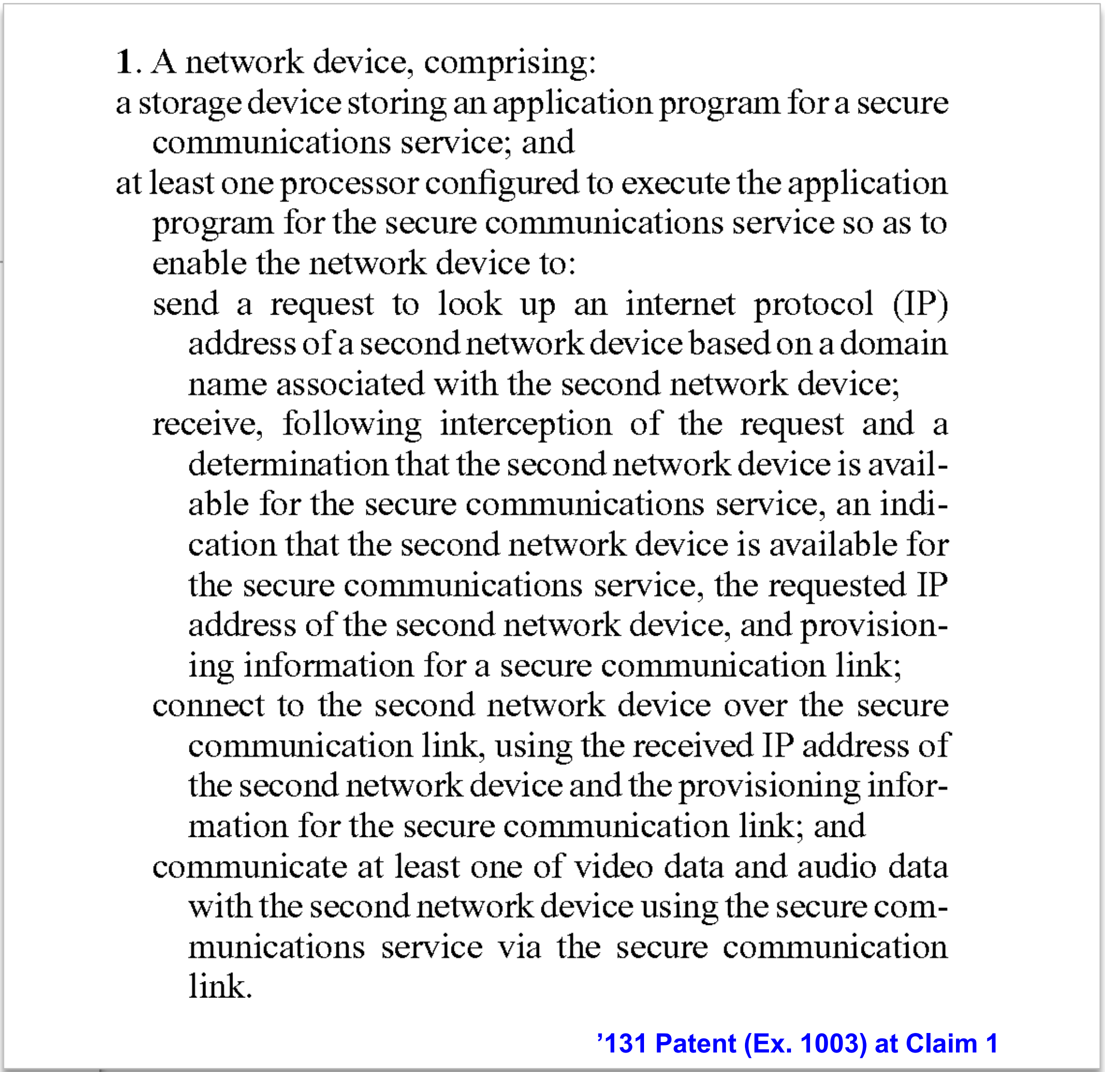
Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

A network device comprises a storage device storing an application program for a secure communications service; and at least one processor configured to execute the application program enabling the network device to: (a) send a request to look up a network address of a second network device based on an identifier; (b) receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a secure communication link; (c) connect to the second network device over the secure communication link, using the received network address of the second network device and the provisioning information for the secure communication link; and (d) communicate at least one of video data and audio data with the second network device using the secure communications service via the secure communication link.

27 Claims, 40 Drawing Sheets

Petitioner Apple Inc. - Exhibit 1003, p. 1



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 request to look up an internet protocol (IP) address of a second network device based on a domain name associated with the second network device;

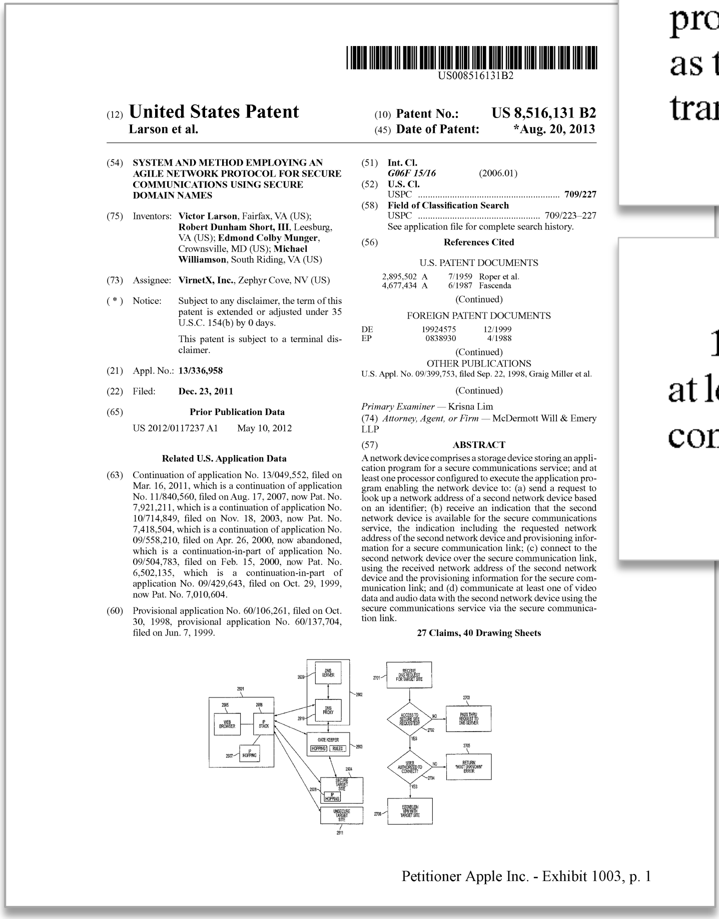
receive, following interception of the request and a determination that the second network device is available for the secure communications service, an indication that the second network device is available for the secure communications service, the requested IP address of the second network device, and provisioning information for a secure communication link;

connect to the second network device over the secure communication link, using the received IP address of the second network device and the provisioning information for the secure communication link; and

communicate at least one of video data and audio data with the second network device using the secure communications service via the secure communication link.

’131 Patent (Ex. 1003) at Claim 1

’131 Patent, Claim 2, 3, and 16



US008516131B2

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

(10) **Patent No.: US 8,516,131 B2**
(45) **Date of Patent: *Aug. 20, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,958**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0117237 A1 May 10, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,677,434	A	6/1987	Fascenda

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

U.S. Appl. No. 09/399,753, filed Sep. 22, 1998, Graig Miller et al.

(Continued)

Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

A network device comprises a storage device storing an application program for a secure communications service; and at least one processor configured to execute the application program enabling the network device to: (a) send a request to look up a network address of a second network device based on an identifier; (b) receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a secure communication link; (c) connect to the second network device over the secure communication link, using the received network address of the second network device and the provisioning information for the secure communication link; and (d) communicate at least one of video data and audio data with the second network device using the secure communications service via the secure communication link.

27 Claims, 40 Drawing Sheets

Petitioner Apple Inc. - Exhibit 1003, p. 1

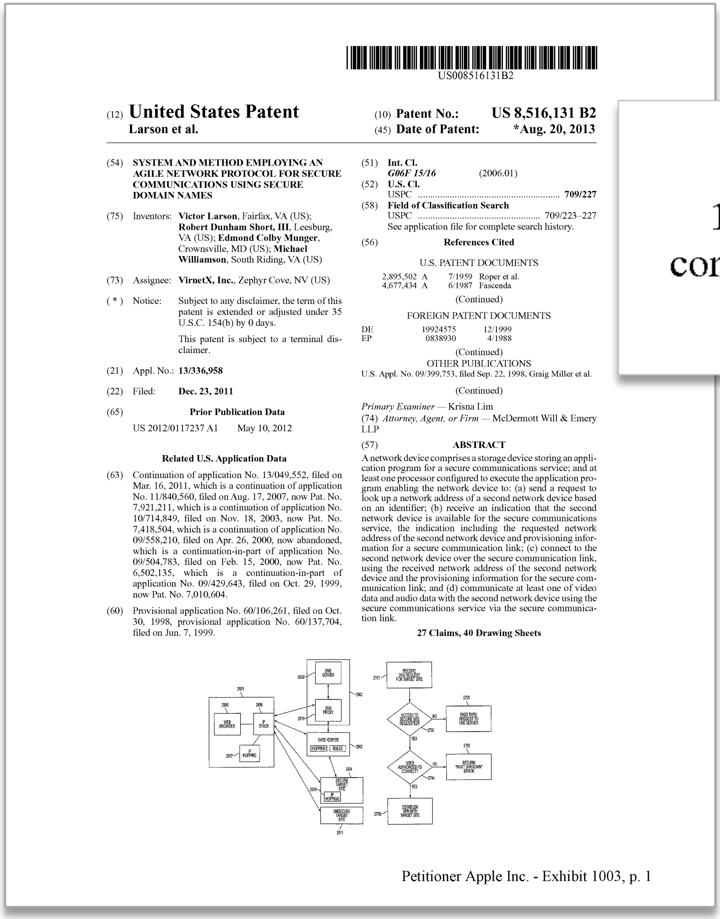
2. The network device of claim **1**, wherein the secure communications service includes an audio-video conferencing service.

3. The network device of claim **2**, wherein the at least one processor is configured to execute the application program so as to encrypt at least one of the video data and the audio data transmitted over the secure communication link.

16. The method of claim **15**, further comprising encrypting at least one of the video data and the audio data over the secure communication link.

’131 Patent (Ex. 1003) at Claim 2, 3, and 16

’131 Patent, Claim 10



US008516131B2

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

(10) **Patent No.:** **US 8,516,131 B2**
(45) **Date of Patent:** ***Aug. 20, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/336,958**

(22) Filed: **Dec. 23, 2011**

(65) **Prior Publication Data**

US 2012/0117237 A1 May 10, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,677,434	A	6/1987	Fascenda

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

U.S. Appl. No. 09/399,753, filed Sep. 22, 1998, Graig Miller et al.

(Continued)

Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

A network device comprises a storage device storing an application program for a secure communications service; and at least one processor configured to execute the application program enabling the network device to: (a) send a request to look up a network address of a second network device based on an identifier; (b) receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a secure communication link; (c) connect to the second network device over the secure communication link, using the received network address of the second network device and the provisioning information for the secure communication link; and (d) communicate at least one of video data and audio data with the second network device using the secure communications service via the secure communication link.

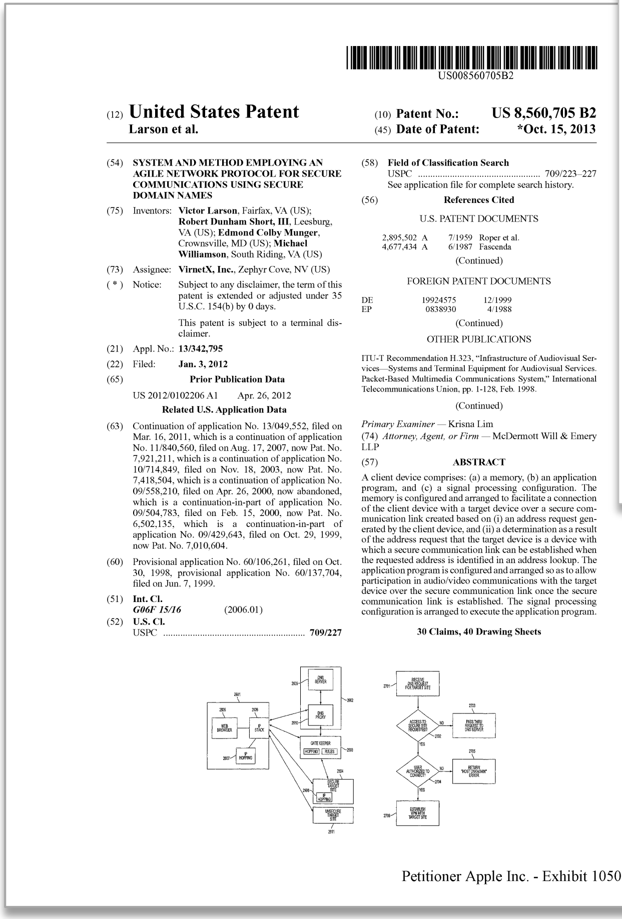
27 Claims, 40 Drawing Sheets

Petitioner Apple Inc. - Exhibit 1003, p. 1

10. The network device of claim **1**, wherein the secure communication link is a virtual private network link.

’131 Patent (Ex. 1003) at Claim 10

’705 Patent, Claim 16



US008560705B2

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

(10) **Patent No.:** **US 8,560,705 B2**
(45) **Date of Patent:** ***Oct. 15, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/342,795**

(22) Filed: **Jan. 3, 2012**

(65) **Prior Publication Data**

US 2012/0102206 A1 Apr. 26, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,677,434	A	6/1987	Fascenda

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

ITU-T Recommendation H.323, “Infrastructure of Audiovisual Services—Systems and Terminal Equipment for Audiovisual Services. Packet-Based Multimedia Communications System,” International Telecommunications Union, pp. 1-128, Feb. 1998.

(Continued)

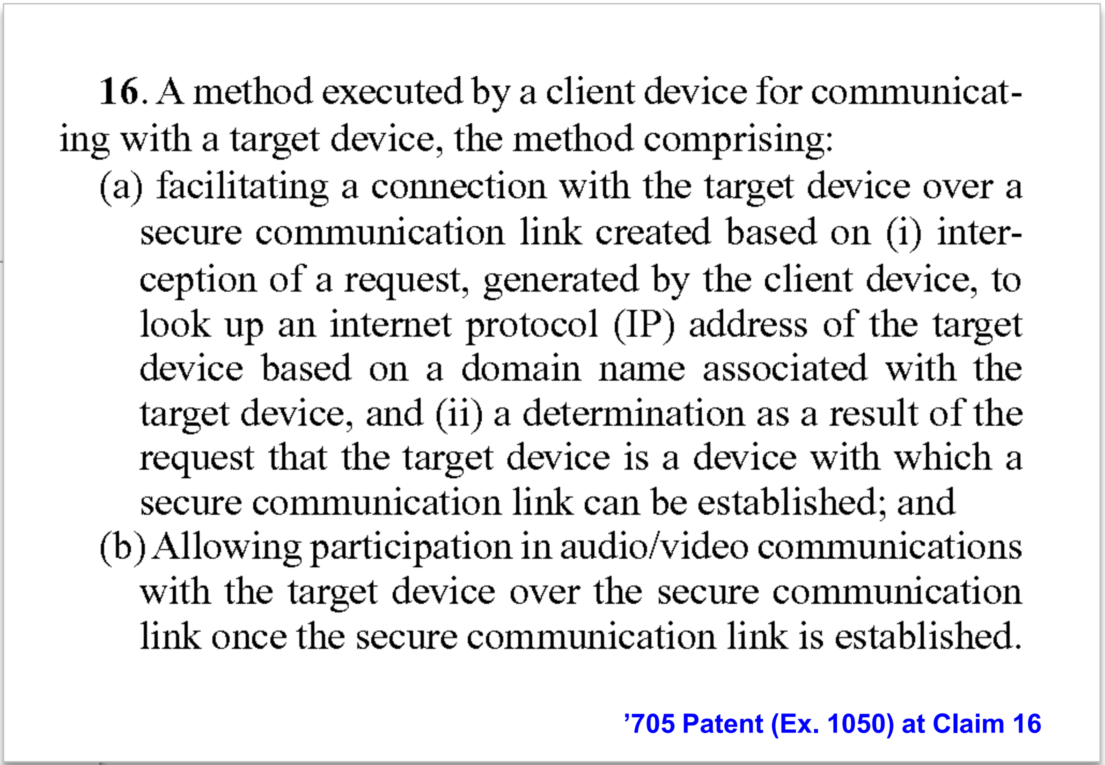
Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

A client device comprises: (a) a memory, (b) an application program, and (c) a signal processing configuration. The memory is configured and arranged to facilitate a connection of the client device with a target device over a secure communication link created based on (i) an address request generated by the client device, and (ii) a determination as a result of the address request that the target device is a device with which a secure communication link can be established when the requested address is identified in an address lookup. The application program is configured and arranged so as to allow participation in audio/video communications with the target device over the secure communication link once the secure communication link is established. The signal processing configuration is arranged to execute the application program.

30 Claims, 40 Drawing Sheets

Petitioner Apple Inc. - Exhibit 1050, p. 1



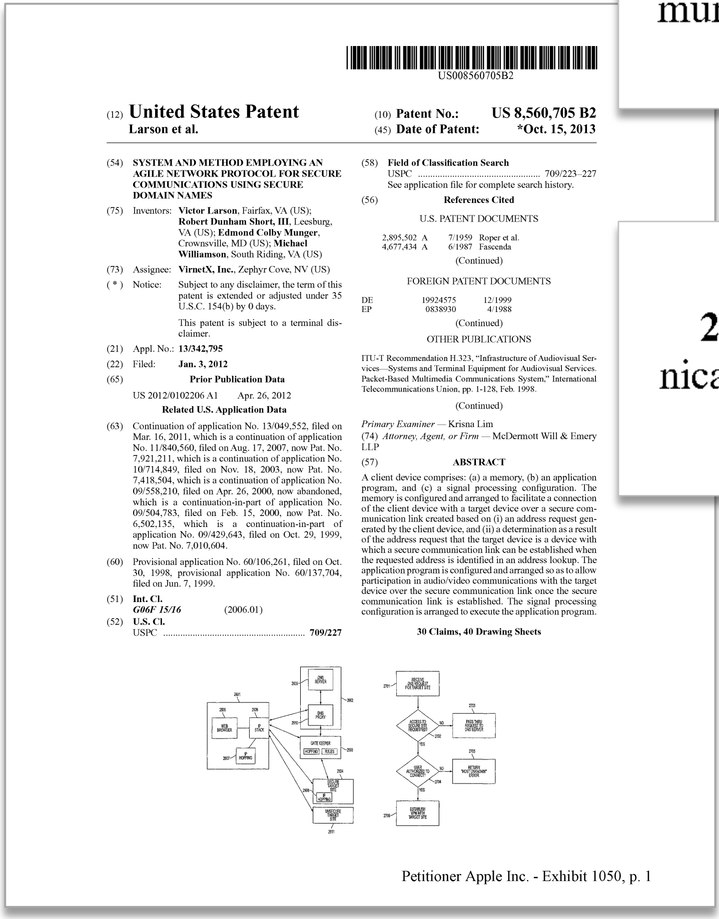
16. A method executed by a client device for communicating with a target device, the method comprising:

(a) facilitating a connection with the target device over a secure communication link created based on (i) interception of a request, generated by the client device, to look up an internet protocol (IP) address of the target device based on a domain name associated with the target device, and (ii) a determination as a result of the request that the target device is a device with which a secure communication link can be established; and

(b) Allowing participation in audio/video communications with the target device over the secure communication link once the secure communication link is established.

’705 Patent (Ex. 1050) at Claim 16

’705 Patent, Claim 3, 6, and 21



US008560705B2

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

(10) **Patent No.: US 8,560,705 B2**
(45) **Date of Patent: *Oct. 15, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/342,795**

(22) Filed: **Jan. 3, 2012**

(65) **Prior Publication Data**

US 2012/0102206 A1 Apr. 26, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,677,434	A	6/1987	Fascenda

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

ITU-T Recommendation H.323, “Infrastructure of Audiovisual Services—Systems and Terminal Equipment for Audiovisual Services. Packet-Based Multimedia Communications System,” International Telecommunications Union, pp. 1-128, Feb. 1998.

(Continued)

Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

A client device comprises: (a) a memory, (b) an application program, and (c) a signal processing configuration. The memory is configured and arranged to facilitate a connection of the client device with a target device over a secure communication link created based on (i) an address request generated by the client device, and (ii) a determination as a result of the address request that the target device is a device with which a secure communication link can be established when the requested address is identified in an address lookup. The application program is configured and arranged so as to allow participation in audio/video communications with the target device over the secure communication link once the secure communication link is established. The signal processing configuration is arranged to execute the application program.

30 Claims, 40 Drawing Sheets

Petitioner Apple Inc. - Exhibit 1050, p. 1

3. The client device of claim **1**, wherein the client device is a phone.

6. The client device of claim **3**, wherein the secure communication link is a virtual private network link.

21. The method of claim **16**, wherein the secure communication link is a virtual private network link.

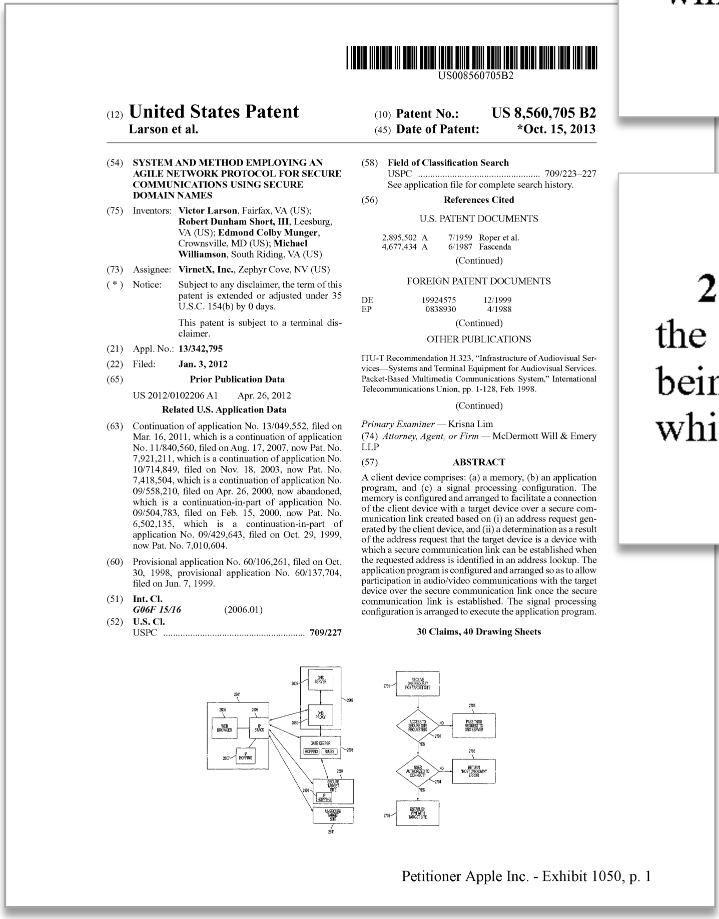
’705 Patent (Ex. 1050) at Claim 3, 6, and 21

’705 Patent, Claim 4 and 20

4. The client device of claim **3**, wherein the establishment of the secure communication link is based on a determination being made by a server that the target device is a device with which a secure communication link can be established.

20. The method of claim **16**, wherein the establishment of the secure communication link is based on a determination being made by a server that the target device is a device with which a secure communication link can be established.

’705 Patent (Ex. 1050) at Claim 4 and 20



US008560705B2

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

(10) **Patent No.:** **US 8,560,705 B2**
(45) **Date of Patent:** ***Oct. 15, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/342,795**

(22) Filed: **Jan. 3, 2012**

(65) **Prior Publication Data**

US 2012/0102206 A1 Apr. 26, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,677,434	A	6/1987	Fascenda

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

ITU-T Recommendation H.323, “Infrastructure of Audiovisual Services—Systems and Terminal Equipment for Audiovisual Services. Packet-Based Multimedia Communications System,” International Telecommunications Union, pp. 1-128, Feb. 1998.

(Continued)

Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

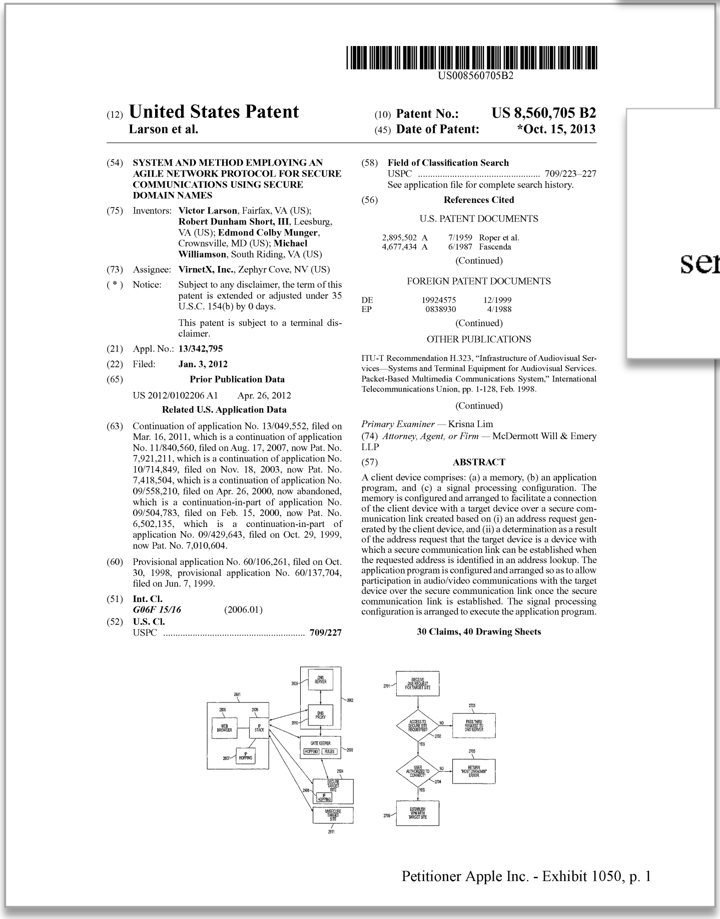
A client device comprises: (a) a memory, (b) an application program, and (c) a signal processing configuration. The memory is configured and arranged to facilitate a connection of the client device with a target device over a secure communication link created based on (i) an address request generated by the client device, and (ii) a determination as a result of the address request that the target device is a device with which a secure communication link can be established when the requested address is identified in an address lookup. The application program is configured and arranged so as to allow participation in audio/video communications with the target device over the secure communication link once the secure communication link is established. The signal processing configuration is arranged to execute the application program.

30 Claims, 40 Drawing Sheets

Petitioner Apple Inc. - Exhibit 1050, p. 1

’705 Patent, Claim 13 and 28

13. The client device of claim 3, wherein the target device is a server.



US008560705B2

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

(10) **Patent No.: US 8,560,705 B2**
(45) **Date of Patent: *Oct. 15, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmond 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.: **13/342,795**

(22) Filed: **Jan. 3, 2012**

(65) **Prior Publication Data**

US 2012/0102206 A1 Apr. 26, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/049,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502	A	7/1959	Roper et al.
4,677,434	A	6/1987	Fascenda

(Continued)

FOREIGN PATENT DOCUMENTS

DE	19924575	12/1999
EP	0838930	4/1988

(Continued)

OTHER PUBLICATIONS

ITU-T Recommendation H.323, “Infrastructure of Audiovisual Services—Systems and Terminal Equipment for Audiovisual Services. Packet-Based Multimedia Communications System,” International Telecommunications Union, pp. 1-128, Feb. 1998.

(Continued)

Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

A client device comprises: (a) a memory, (b) an application program, and (c) a signal processing configuration. The memory is configured and arranged to facilitate a connection of the client device with a target device over a secure communication link created based on (i) an address request generated by the client device, and (ii) a determination as a result of the address request that the target device is a device with which a secure communication link can be established when the requested address is identified in an address lookup. The application program is configured and arranged so as to allow participation in audio/video communications with the target device over the secure communication link once the secure communication link is established. The signal processing configuration is arranged to execute the application program.

30 Claims, 40 Drawing Sheets

Petitioner Apple Inc. - Exhibit 1050, p. 1

28. The method of claim 16, wherein the target device is a server.

’705 Patent (Ex. 1050) at Claim 13 and 28