IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Munger *et al.*
U.S. Patent No.: 6,502,135 Attorney Docket No.: 38868-0004IP1
Issue Date: Dec. 31, 2002
Appl. Serial No.: 09/504,783
Filing Date: Feb. 15, 2000
Title: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT NO. 6,502,135 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42

TABLE OF CONTENTS

EXHIBITS

MSFT-1001	U.S. Patent No. 6,502,135 to Munger *et al.* ("the '135 patent")
MSFT-1002	Excerpts from the Prosecution History of the '135 Patent ("the Prosecution History")
MSFT-1003	Declaration of Dr. Roch Guerin re '135
MSFT-1004	(Reserved)
MSFT-1005	Declaration of Chris A. Hopen re '135
MSFT-1006	Declaration of James Chester re '135
MSFT-1007	Aventail Connect v3.01/2.51 Administrator's Guide and Aventail ExtraNet Server v3.0 Administrator's Guide (UNIX and Windows NT) (1996-1999)
MSFT-1008	(Reserved)
MSFT-1009	(Reserved)
MSFT-1010	(Reserved)
MSFT-1011	(Reserved)
MSFT-1012	(Reserved)
MSFT-1013	(Reserved)
MSFT-1014	(Reserved)
MSFT-1015	(Reserved)

MSFT-1016	Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities," November 1987
MSFT-1017	Mockapetris, P., RFC 1035, "Domain Names – Implementation and Specification," November 1987
MSFT-1018	(Reserved)
MSFT-1019	(Reserved)
MSFT-1020	(Reserved)
MSFT-1021	Aventail AutoSOCKS v2.1 Administration and User's Guide, 1996-1997
MSFT-1022	Aventail Connect v3.1/v2.6 Administrator's Guide, 1996-1999
MSFT-1023	(Reserved)
MSFT-1024	(Reserved)
MSFT-1025	(Reserved)
MSFT-1026	(Reserved)
MSFT-1027	(Reserved)
MSFT-1028	(Reserved)
MSFT-1029	(Reserved)
MSFT-1030	(Reserved)
MSFT-1031	(Reserved)
MSFT-1032	(Reserved)
MSFT-1033	(Reserved)

MSFT-1034	(Reserved)
MSFT-1035	(Reserved)
MSFT-1036	(Reserved)
MSFT-1037	(Reserved)
MSFT-1038	(Reserved)
MSFT-1039	(Reserved)
MSFT-1040	(Reserved)
MSFT-1041	Bradner, S., RFC 2026, "The Internet Standards Process – Revision 3," October 1996
MSFT-1042	(Reserved)
MSFT-1043	(Reserved)
MSFT-1044	(Reserved)
MSFT-1045	Memorandum Opinion in *VirnetX, Inc. v. Microsoft Corporation*, 6:07-CV-80 (7/30/09) (EDTX)
MSFT-1046	VirnetX's Opening Claim Construction Brief in *VirnetX Inc. v. Cisco Systems, Inc., et al.*, 6:10-CV-417 (11/4/11) (EDTX)
MSFT-1047	(Reserved)
MSFT-1048	VirnetX's Reply Claim Construction Brief in *VirnetX Inc. v. Cisco Systems, Inc., et al.*, 6:10-CV-417 (12/19/11) (EDTX)
MSFT-1049	Memorandum Opinion and Order in *VirnetX Inc. v. Cisco Systems, Inc., et al.*, 6:10-CV-417 (4/25/12) (EDTX)
MSFT-1050	(Reserved)

MSFT-1051	(Reserved)
MSFT-1052	(Reserved)
MSFT-1053	(Reserved)
MSFT-1054	(Reserved)
MSFT-1055	(Reserved)
MSFT-1056	(Reserved)
MSFT-1057	Curriculum Vitae of Chris Hopen
MSFT-1058	"Aventail Ships the First Standards-Based Virtual Private Network Software Solution," PR Newswire, PR Newswire Association LLC, May 2, 1997
MSFT-1059	Szeto, L., "Aventail delivers highly secure, flexible VPN solution," InfoWorld Media Group, June 23, 1997
MSFT-1060	"Aventail Introduces the First Extranet-Ready Platform; Aventail Previews its Latest Solution, Aventail ExtraNet Center, at Networld+Interop in Atlanta," PR Newswire, PR Newswire Association LLC, October 12, 1998
MSFT-1061	(Reserved)
MSFT-1062	Curriculum Vitae of James Chester
MSFT-1063	(Reserved)
MSFT-1064	(Reserved)
MSFT-1065	(Reserved)

MSFT-1066	Takahiro Kiuchi and Shigekoto Kaihara, "C-HTTP - The Development of a Secure, Closed HTTP-based Network on the Internet," published by IEEE in the Proceedings of SNDSS 1996
MSFT-1067	(Reserved)
MSFT-1068	D. Eastlake, RFC 2535, "Domain Name System Security Extensions," (March 1999)
MSFT-1069	IPR2013-00348, Patent Owner's Preliminary Response
MSFT-1070	(Reserved)
MSFT-1071	(Reserved)
MSFT-1072	Dismissal without prejudice with regard to invalidity of *VirnetX Inc. v.Microsoft Corp.*, Docket No. 6:07CV80
MSFT-1073	Dismissal from *VirnetX Inc. v. Microsoft Corp.*, Docket No. 6:10CV94
MSFT-1074	Copy of Docket from *VirnetX Inc. v. Microsoft Corp.*, Docket No. 6:10CV94
MSFT-1075	Redacted Settlement Agreement between VirnetX Inc. and Microsoft Corporation (Exhibit 10.1 from VirnetX SEC filing)

Microsoft Corporation ("Petitioner" or "Microsoft") petitions for *Inter Partes* Review ("IPR") under 35 U.S.C. §§ 311–319 and 37 C.F.R. § 42 of claims 1, 3, 4, 7, 8, 10, 12, and 13 ("the Challenged Claims") of U.S. Patent No. 6,502,135 ("the '135 patent"). As explained in this petition, there exists a reasonable likelihood that Microsoft will prevail with respect to at least one of the Challenged Claims.

The Challenged Claims are unpatentable based on teachings set forth in at least the references presented in this petition. Microsoft respectfully submits that an IPR should be instituted, and that the Challenged Claims should be canceled as unpatentable.

I. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Petitioner, Microsoft Corporation, is the real party-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '135 patent is the subject of a number of civil actions including: (i) Civ. Act. No. 6:13-cv-00211-LED (E.D. Tex.), filed February 26, 2013; (ii) Civ. Act. No. 6:12-cv-00855-LED (E.D. Tex.), filed November 6, 2012; (iii) Civ. Act. No. 6:10-cv-00417-LED (E.D. Tex.), filed August 11, 2010; (iv) Civ. Act. No. 6:11-cv-00018-LED (E.D. Tex), (iv) Civ. Act. No. 6:13-cv-00351-LED (E.D. Tex), filed April 22, 2013 ("the 2013 VirnetX litigation"); (v) Civ. Act. No. 6:10-cv-00094 (E.D. Tex); and (vi) Civ. Act. No. 6:07-cv-00080 (E.D. Tex).

The '135 patent is the subject of two petitions for *inter partes* review filed by RPX Corporation, which have been designated as IPR2014-00171 and IPR2014-00172. The

'135 patent is also the subject of merged *inter partes* reexamination nos. 95/001,679 and 95/001,682. In the merged proceedings, the Office recently issued a Non-Final Action rejecting all 18 claims of the '135 patent, including rejections based on, *inter alia*, Ex. 1007 (Aventail) and Ex. 1066 (Kiuchi). The '135 patent also was subject to reexamination no. 95/001,269, which concluded on June 7, 2011 with an inter partes reexamination certificate confirming all claims and adding new claim 18.

Concurrently with this petition, Microsoft is filing another petition for IPR (identified with attorney docket number 38868-0003IP2) of the '135 patent. The relationship between the limited grounds presented in these two petitions is discussed in Section VI.

C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Microsoft provides the following designation of counsel.

LEAD COUNSEL	BACKUP COUNSEL
W. Karl Renner, Reg. No. 41,265 3200 RBC Plaza 60 South Sixth Street Minneapolis, MN 55402 T: 202-783-5070 F: 202-783-2331	Kevin E. Greene, Reg. No. 46,031 3200 RBC Plaza 60 South Sixth Street Minneapolis, MN 55402 T: 202-626-6376 F: 202-783-2331

D. Service Information

Please address all correspondence and service to counsel at the address provided in Section I(C). Microsoft also consents to electronic service by email at IPR38868-0004IP1@fr.com.

II. PAYMENT OF FEES – 37 C.F.R. § 42.103

Microsoft authorizes the Patent and Trademark Office to charge Deposit Account No.

06-1050 for the fee set in 37 C.F.R. § 42.15(a) for this Petition and further authorizes payment for any additional fees to be charged to this Deposit Account.

III. REQUIREMENTS FOR IPR UNDER 37 C.F.R. § 42.104

A. Grounds for Standing Under 37 C.F.R. § 42.104(a)

Microsoft certifies that the '135 Patent is eligible for IPR. The present petition is being filed within one year of service of a complaint against Microsoft in the 2013 VirnetX litigation.[1]

VirnetX has asserted the '135 patent against Microsoft. Under the plain language of the statute, Microsoft's petition is timely. Out of an abundance of caution, however, Microsoft explains herein why VirnetX's prior assertions do not impact Microsoft's ability to bring the current IPR. Chief among these, (1) dismissal of Microsoft's validity challenges in the prior disputes was *without prejudice* to Microsoft's rights to challenge again; and (2) Microsoft agreed to the prior dismissals were based on VirnetX's dismissal, settlement, release and license (all of which VirnetX has ignored to sue Microsoft again).

Contextually, in two prior instances, VirnetX asserted the '135 patent against Microsoft: *VirnetX Inc. v. Microsoft Corp.*, Docket Nos. 6:07CV80 and 6:10CV94 ("the 2007

[1]The complaint in the 2013 VirnetX litigation was served on April 23, 2013.

VirnetX litigation" and "the 2010 VirnetX litigation," respectively)[2]. Neither these litigations nor service of corresponding complaints bar Microsoft from petitioning for IPR of the '135 patent under 35 U.S.C. § 315(b) for at least the following reasons.

1) In agreeing to voluntarily dismiss the 2007 and 2010 VirnetX litigations, both parties stipulated that Microsoft's defense of invalidity was dismissed *without prejudice*, nullifying effect of the service of corresponding complaints for purposes of the applicable rules. *See* Ex. 1075, § 5.1. And, based on the "without prejudice" language, as well as on the licenses, releases, and other language of the settlements, Microsoft withdrew its challenges to the patent without prejudice to the right to bring them in the future.
2) Independent of considerations relating to dismissal and nullification of the service in the 2007 and 2010 VirnetX litigations, proper interpretation of 35 U.S.C. § 315(b) permits this IPR under the present circumstances.

1. Voluntarily dismissal of invalidity without prejudice of the 2007 and 2010 VirnetX litigations nullifies service of corresponding complaints for purposes of 35 U.S.C. § 315(b).

In the 2007 and 2010 VirnetX litigations, VirnetX voluntarily dismissed its infringement actions, pursuant to Fed. R. Civ. P. 41, before entry of a final judgment. The Board

[2] The 2007 and 2010 VirnetX litigations accused Microsoft of infringement of both U.S. Patent Nos. 6,502,135 and 7,188,180.

has previously found that, in appropriate circumstances, "a voluntary dismissal of an infringement action [nullifies] the effect of the alleged service of the complaint on the petitioner." IPR2013-00175 (*BAE Systems Information and Electronic Systems Integration, Inc. v. Cheetah Omni*, *LLC*), Paper 15 at 3. Even voluntary dismissal of an infringement action *with* prejudice – a situation that indicates a far more definitive resolution of an invalidity challenge – has been found to nullify the legal effect of service of a corresponding complaint so long as there is a reason "why the dismissal with prejudice should be treated as a dismissal without prejudice." IPR2013-00168 (*Universal Remote Control, Inc. v. Universal Electronics, Inc.*), Paper 9 at 6. Based on the facts of this case, the dismissals of the infringement actions in the 2007 and 2010 VirnetX litigations should indeed be treated as dismissals without prejudice as to invalidity for purposes of 35 U.S.C. § 315(b).

Here, the Court dismissed the 2007 and 2010 VirnetX litigations pursuant to a settlement agreement that expressly preserved Microsoft's ability to later challenge the validity of the patents-in-suit. The settlement agreement states, "Microsoft's affirmative defenses and counterclaims of (i) non-infringement and invalidity shall be dismissed <u>without prejudice</u>". Ex. 1075, at § 5.1. Consistent with this, the Court dismissed the 2007 case, complementing its indication that "[a]ll claims asserted [by VirnetX] against Microsoft . . . are dismissed with prejudice" with overt recognition of Microsoft's continued ability to challenge validity. Ex. 1072, at p. 1 ("dismissal is <u>without prejudice</u> to Microsoft's ability to assert, in future actions, (i) affirmative defenses and/or counterclaims of invalidity or non-

infringement." (emphasis added)).

With regard to the 2010 case, invalidity had not yet been raised, as Microsoft had not yet filed an answer to VirnetX's complaint at the time of its dismissal. *See* Ex. 1074, at pp. 2-3. Without any affirmative defenses and/or counterclaims having been asserted by Microsoft, the Court had no basis to include the defenses and counterclaims in its dismissal order. Rather, the Court properly left untouched Microsoft's ability to later raise invalidity challenges in accordance with the settlement agreement (which unambiguously recognizes that the voluntary dismissal was without prejudice on invalidity in *both* the 2007 and 2010 VirnetX litigations). Congruently, the settlement agreement adds that Microsoft "does not release or discharge (or grant a covenant or hold harmless as to) its Claims that the Licensed Patents are invalid." Ex. 1075, § 3.2.

In exchange for retaining its right to later challenge the validity of the '135 patent, Microsoft agreed to discontinue all of its then-pending challenges to the patents-in-suit in the Patent Office. Microsoft agreed to stop its participation in the then pending *inter partes* reexamination of the '135 patent that Microsoft had requested. *See* Ex. 1075, § 7.16. To that end, and in accordance with the agreement, Microsoft filed "with the United States Patent and Trademark Office notifications in the then-current reexamination proceedings of the Patents-In-Suit indicating that Microsoft Corporation will not participate in those reexamination proceedings." Ex. 1075, § 7.16. And, Microsoft has not challenged the validity of the '135 patent since the settlement of the 2007 and 2010 VirnetX litigations. Only now, in re-

sponse to VirnetX once again suing Microsoft, does Microsoft seek to exercise the right that it earlier preserved to challenge the validity of the '135 patent.

Importantly, the "without prejudice" manner in which Microsoft's affirmative defenses and counterclaims were dismissed placed Microsoft and VirnetX in the same position as to invalidity that they would have been had the earlier invalidity action never been brought. *See* IPR2013-00168 (*Universal Remote Control, Inc. v. Universal Electronics, Inc.*), Paper 9 at 6 Microsoft does not seek a broad ruling that automatically treats every voluntary dismissal as nullifying the effect of service for *inter partes* review purposes. Rather, Microsoft respectfully submits that the particular circumstances of *this case* simply warrant such treatment. Because the prior dismissals did not prejudice Microsoft's right to challenge validity, and because VirnetX can hardly claim harassment by way of administrative challenges uncoordinated with litigation, the circumstances here – where a patentee has sued on the same patents again after settling prior disputes and granting a license – justify allowing Microsoft to test the validity of the patents. Microsoft presently faces a third assertion by VirnetX of the '135 patent, and Microsoft earlier withdrew its validity challenge based on an agreement in which VirnetX overtly acknowledged (and thus, preserved) Microsoft's ability to later challenge the '135 patent. These facts make it appropriate to treat the dismissal of the 2007 and 2010 VirnetX litigations as nullifying earlier service for purposes of § 315(b), making IPR available to Microsoft in this instance.

2. Independent of considerations relating to dismissal of the 2007 and 2010 VirnetX litigations, proper interpretation of 35

U.S.C. § 315(b) permits this IPR under the present circumstances

If for any reason the Board decides that the dismissal of the prior litigations does not nullify the effect of service, the Board should nevertheless interpret 35 U.S.C. § 315(b) as permitting this IPR since the Petition is being filed within one year of service of **a** complaint. Notably, § 315(b) does not specify a one-year deadline that runs from the date of the first complaint served on a petitioner. Rather, it states "[a]n *inter partes* review may not be instituted if the petition requesting the proceeding is filed more than 1 year after the date on which the petitioner, real party in interest, or privy of the petitioner is served with a complaint alleging infringement of the patent." 35 U.S.C. § 315(b).

Microsoft appreciates that the Board may have found otherwise in *Universal Remote Control* (IPR2013-00168), but Microsoft seeks further consideration of the issue because statutory inclusion of the indefinite article "a" before the subject—"complaint"—creates an ambiguity in the application of § 315(b) to the current situation – where an IPR is filed within one year of service of a subsequent complaint alleging infringement of the patent, but after one year from service of an initial complaint(s) alleging infringement of the same patent. *See* IPR2013-00168 (*Universal Remote Control, Inc. v. Universal Electronics, Inc.*), Paper 9 at 5. Here, multiple complaints alleging infringement by Microsoft of the same patent unquestionably creates multiple dates of service from which the preclusive effect of § 315(b) may be measured, and the later date is within one year of the present Petition in compliance with §315(b), if the most recent complaint is recognized as "a complaint alleging infringe-

ment of the patent."

The *Universal Remote Control* Board acknowledged that "the plain language of the statute does not address the subject of multiple lawsuits involving the same patent." *Id.* at p. 4. Yet, that Board declined an invitation to interpret the statute, suggesting to the contrary that statute was in fact not subject to interpretation, despite the ambiguity inherent in the language of § 315(b).

In as much as the § 315(b) language is open to competing interpretations that materially impact its application to the present case, Microsoft believes that § 315(b) is necessarily open to interpretation, and Microsoft hereby requests the same. In doing so, Microsoft advances the potential for at least the following two interpretations, while submitting that the second is more appropriate under the circumstances:

(1) If "a complaint" is interpreted to mean "a first complaint," then § 315(b) would be read: "An *inter partes* review may not be instituted if the petition requesting the proceeding is filed more than 1 year after the date on which the petitioner, real party in interest, or privy of the petitioner is served with a first complaint alleging infringement of the patent."

(2) If "a complaint" is interpreted to mean "any complaint" including "a latest filed complaint," then § 315(b) would be read: "An *inter partes* review may not be instituted if the petition requesting the proceeding is filed more than 1 year after the date on which the petitioner, real party in interest, or privy of the petitioner is

served with a latest complaint alleging infringement of the patent."

In any event, as can be seen from each potential interpretation, "a complaint" leaves § 315(b) open to various competing interpretations, and thus, is not sufficient to avoid the need for interpretation.

It has been noted that "because most of the elements of these new proceedings are required to be implemented through regulations, the USPTO also has substantial discretion in construing and applying the statutory text of chapters 31 and 32." Joe Matal, *A Guide to the Legislative History of the America Invents Act: Part II of II*, 21 Fed. Cir. Bar J. 539, 604-5 (2012). Given this authority, the Board should adopt the second potential interpretation of § 315(b), which would permit institution of an IPR where the petition is filed within one year of service of any complaint alleging infringement of the patent. This interpretation is consistent with the legislative history, which reveals Congresses mutual goals of preventing "abusive serial challenges to patents" while "coordinat[ing] *inter partes* and post-grant review with litigation." 157 Con. Rec. S1041 (daily ed. Mar. 1, 2011) (statement of Sen. Kyl). Indeed, under this proposed interpretation, a patentee would only be subject to challenge when bringing a complaint against a party, leaving them in full control over the situation, and preventing the kind of abusive challenges that Congress intended to shut down. To the point, when considering the various post-grant challenges included in the proposed legislation, the House of Representatives' Committee on the Judiciary more specifically reported:

The Committee recognizes the importance of quiet title to patent owners to

> ensure continued investment resources. While this amendment is intended to remove current disincentives to current administrative processes, the changes made by it are not to be used as tools for harassment or a means to prevent market entry through repeated litigation and administrative attacks on the validity of a patent. Doing so would frustrate the purpose of the section as providing quick and cost effective alternatives to litigation. Further, such activity would divert resources from the research and development of inventions. As such, the Committee intends for the USPTO to address potential abuses and current inefficiencies under its expanded procedural authority.

H.R. Rep. No. 112-98, 112th Cong., at 76 (2011).

And yet, the patentee's interests were not the only interests of Congressional concern. Congress also clearly intended to provide a quick and cost effective tool for defendants to use as an alternative to litigation. Congress didn't express any intent to limit the use of this tool by defendants, other than to prevent the aforementioned harassment of patentee. Thus, the Board should interpret the statutory limits on IPRs (e.g., the limits imposed by § 315(b)) as safe guards against abusive challenges aimed at harassing a patent owner and not as a means of precluding defendants from using otherwise available tools when confronted with new assertions of infringement, especially when patentees can hardly proclaim harassment when their new complaint of infringement triggers the availability of the tool.

Adopting the proposed interpretation of § 315(b) satisfies these legislative goals. In particular, the proposed interpretation would prevent an IPR from being instituted more than one year after service of a first complaint, unless patentee brings new allegations of in-

fringement against a defendant. By barring an IPR more than a year after service of a first complaint, without regard to service of subsequent complaints, a third party is disincentivised from settling in a manner that promotes dismissal with prejudice; indeed, since such a bar may prevent a party seeking to settle with prejudice from being able to settle without jeopardizing their ability to later use USPTO tools to defend themselves if patentee dishonors the settlement terms. On the other hand, allowing an IPR to be filed within a year of service of any subsequent complaints would coordinate IPR with subsequent litigation and provide the third party with the cost-effective alternative intended by Congress.

Applying the proposed interpretation of § 315(b) to the facts of this case provides a model of how the proposed interpretation aligns with Congressional intent. As described above, the settlement agreement that was mutually reached by the parties in the 2007 and 2010 VirnetX litigations specifically preserved Microsoft's right to challenge the validity of the '135 patent in future proceedings. In other words, the Patent Owner in this case specifically consented to future challenges to the validity of the '135 patent. Therefore, the institution of an IPR as a result of this petition cannot be considered abusive or harassing, because the patent owner has implicitly consented to such a challenge.

One can easily imagine other situations that unjustly frustrate Congressional intent if §315(b) were interpreted inconsistent with Microsoft's proposed interpretation. For example, consider a situation in which a patent owner brings a first complaint alleging infringement of a patent by a defendant's first product. The defendant determines that it has a very

strong argument for non-infringement with regard to the first product. To conserve resources, the defendant decides to focus its defense exclusively on non-infringement. However, the patent owner subsequently brings a second complaint alleging infringement of the same patent by a second product produced by the defendant. In analyzing the patent with regard to the second product, the defendant determines that it does not have a strong argument for non-infringement this time. In this situation, the defendant would not be barred from asserting invalidity of the patent at the second trial, and, for similar reasons, the defendant should not be precluded from pursuing an IPR of the patent owner's patent.

For at least these reasons, Microsoft submits that §315(b) is ambiguous when applied to the situation where multiple lawsuits involve the same patent and therefore should be interpreted as permitting this Petition in light of congressional intent.

B. Identification of Claims Being Challenged (37 C.F.R. § 42.104(b))

Claims 1, 3, 4, 7, 8, 10, 12, and 13 of the '135 patent are unpatentable as being anticipated under 35 U.S.C. § 102(a), (b), & (e), and/or for being obvious over the prior art under 35 U.S.C. § 103. Specifically:

GROUND 1 - Claims 1, 3, 4, 7, 8, 10, 12, and 13 are anticipated under § 102(b) by Aventail Connect v 3.01/2.5 Administrator's Guide ("Aventail") (Ex. 1007);

GROUND 2 - Claims 1, 3, 4, 7, 8, 10, 12, and 13 are obvious under § 103 based on Aventail (Ex. 1007);

GROUND 3 - Claim 4 is obvious under § 103 based on Aventail (Ex. 1007) in view of RFC 1035 (Ex. 1017);

GROUND 4 - Claims 1, 3, 4, 7, 8, 10, and 12 are anticipated under § 102(b) by Takahiro Kiuchi and Shigekoto Kaihara, "C-HTTP - The Development of a Secure, Closed HTTP-based Network on the Internet," the Proceedings of SNDSS 1996 ("Kiuchi") (Ex. 1066);

GROUND 5 - Claim 8 is obvious under § 103 based on Kiuchi (Ex. 1066) in view of RFC 1034 (Ex. 1016).

Petitioner's proposed construction of the contested claims, the evidence relied upon, and the precise reasons why the claims are unpatentable are provided in §§ IV and V, below.

IV. Relevant Information Concerning the Contested Patent

A. Effective Filing Date and Prosecution History of the '135 patent

The '135 patent issued from U.S. Application No. 09/504,783, filed February 15, 2000. The '783 application is a **continuation-in-part** of U.S. Application No. 09/429,653, filed on October 29, 1999. The '783 and '653 applications each attempt to claim priority to Provisional Application Nos. 60/106,261, filed October 30, 1998 and 60/137,704, filed June 7, 1998.

Of the Challenged Claims, claims 1, 10, and 13 are the independent claims. Claims 1 and 10 rely on information first presented in the '783 CIP application. For example, claim

1 specifies "generating from the client computer a **Domain Name Service (DNS) request** …" and subsequent steps involving that DNS request, while claim 10 specifies "[a] system … comprising … a **DNS proxy server**…" Applications filed prior to the '783 application do not contain the term "domain name service" much less describe systems using DNS requests or DNS proxy servers to establish VPNs. Claim 13 likewise relies on information first presented in the '783 application. For example, it specifies "…receiving from one of the plurality of client computers **a request** to establish a connection…" and "…authenticating, with reference to one of the plurality of authentication tables, that **the request** received in step (1) is from an authorized client." Neither step is described in any application filed before the '783 application. Accordingly, the effective filing date of the Challenged Claims is no earlier than February 15, 2000.

B. Construction of Terms Used in the Claims

In an IPR, claims must be given their broadest reasonable construction in light of the specification. 37 C.F.R. § 42.100(b). In view of this, it is reasonable for the Board to consider subject matter that Patent Owner contends infringes the claims, and constructions Patent Owner has advanced in litigation. The words in the claims should be used to determine the broadest reasonable construction. "[I]t is the Patent Owner's burden to precisely define the invention in the claims." *AirCraft Medical LTD. v. Verathon Inc.*, Reexam. Control No. 95/000,161, Appeal 2012-007851, p. 16 (PTAB Dec. 11, 2012) (citing *In re Morris*, 127 F.3d 1048, 1056 (Fed. Cir. 1997)). Of course, the specification must also be consulted to

determine the broadest reasonable construction of the claims.

1. Virtual Private Network (VPN) (Claims 1, 10, and 13)

Petitioner submits that the broadest reasonable construction of "**virtual private network**" or "**VPN**" should be broad enough to encompass "a private network that is configured within a public network."

Patent Owner proposes a construction of "VPN" that differs in two respects; namely, that it requires (i) encryption, and (ii) computers in the VPN to directly communicate with each other. Ex. 1069 at 22. Both positions are inconsistent with the broadest reasonable construction of "VPN."

Initially, the '135 patent does not explicitly define the term "VPN." *See* Ex. 1003 at ¶ 17. However, the '135 patent explains that one can provide data security using "IP hopping" schemes, rather than solely by using encryption. As it states, "Data security is *usually* tackled using some form of data encryption." Ex. 1001 at 1:38-39 (emphasis added). The '135 patent also illustrates use of a quasi-random IP hopping scheme to implement a VPN. *See, e.g.*, *id.* at 23:10-14 ("In a second mode referred to as 'promiscuous per VPN' mode, a small set of fixed hardware addresses are used, with a fixed source/destination hardware address used for all nodes communicating over *a virtual private network*." (Emphasis added)). Moreover, claim 6 relies on this particular embodiment, specifying that step 3 of claim 1 "comprises the step of *establishing the VPN by creating an IP address hopping scheme* between the client computer and the target computer." *Id.* at 47:53-55 (emphasis added); *see*

also id. at 2:25-36 (explaining use of anonymity techniques). Also, the '135 patent explains that "TARP" routers (which do encrypt traffic) are simply one way to implement VPNs. See, *e.g.,* Ex. 1001 at 38:2-5 ("The VPN is *preferably* implemented using the IP address "hop-ping" features of the basic invention described above…" (emphasis added)); *id.* at 2:66-3:29.

To support its contention that a VPN requires encryption Patent Owner points to the term "FreeS/WAN" in one passage of the '135 patent. Ex. 1069 at 23 (citing Ex. 1001 at 37:50-62). That passage, however, does not define *what* a VPN is, but simply explains that RFC 2535 (the "FreeS/WAN" protocol) can be used to implement *one type of a VPN*. *See id.* Notably, Patent Owner does not cite to any passage of RFC 2535 (Ex. 1068) – the publication actually cited in the '135 patent – to support its assertions. This is because RFC 2535 does not even mention the terms "encryption" or "VPN," much less state that a VPN *must* use encryption.

Patent Owner also points to the construction adopted by certain District Courts that a VPN is "a network of computers which privately and directly communicate with each other by encrypting traffic on insecure paths between the computers where the communication is both secure and anonymous." Ex. 1043 at 8. This construction, however, is not the broadest reasonable construction, but reflects the meaning of the term as used in district court litigation; it is not controlling in this proceeding. The broadest reasonable construction of "VPN" thus does not require encryption, but can establish a "private network" using either

encryption or routing techniques, or both.

Patent Owner next contends that a "VPN" requires computers in a VPN to "*directly communicate* with each other." *See e.g.*, Ex. 1046 at 1-3 (emphasis added). In the August 2010 litigation, the Court found that Patent Owner had *disclaimed* VPNs that do not involve "direct communications" between the involved computers. *Id.* at 6; *see* Ex. 1046 at 6-9; Ex. 1048 at 5-7. The Court relied on Patent Owner's statements to the Office during the '269 reexamination proceeding involving the '135 patent to make this determination; specifically, that the '135 claims were not anticipated by the Aventail systems because "computers connected according to Aventail *do not communicate directly with each other*." [3] (Emphasis added). The Court also observed that "…routers, firewalls, and similar servers that participate in typical network communication do not impede 'direct' communication between a client and target computer." Ex. 1049 at 8 (FN2). As Apple previously explained, the Court's finding that Patent Owner disclaimed a *portion of the literal scope of the '135 patent claims* (*i.e.*, that covering VPNs in which computers do not "directly" communicate) means that the '135 claims in *their broadest reasonable construction* must still encompass this subject matter. IPR2013-00349, Petition at 9-11. Patent Owner's prosecution disclaimer is effective in a district court proceeding but not here. *E.g.*, M.P.E.P. § 2111; *id*. at § 2111.01(I) ("Although claims of issued patents are interpreted in light of the specification, prosecution history, prior art and other claims, *this is not the mode of claim interpretation to be applied during examination*."). The broadest reasonable construction of "VPN" therefore encompasses "a

network of computers which privately communicate – directly or otherwise – with each other on insecure paths between the computers where the communication is both secure and anonymous, where the data transferred may or may not be encrypted."

2. DNS Proxy Server (Claims 10, 8)

Patent Owner has elsewhere asserted that the broadest reasonable construction of a "DNS proxy server" is "a computer or program that responds to a domain name inquiry in place of a DNS." *See* Ex. 1046 at 16-17; Ex. 1069 at 32-33. For the purposes of this Petition, Microsoft adopts this construction. Petitioner notes that Patent Owner has admitted that the DNS proxy server can be distributed across different computers or processes under the broadest reasonable construction. *See* Ex. 1069 at 32-33.

V. MANNER OF APPLYING CITED PRIOR ART TO EVERY CLAIM FOR WHICH AN IPR IS REQUESTED, THUS ESTABLISHING A REASONABLE LIKELIHOOD THAT AT LEAST ONE CLAIM OF THE '135 PATENT IS UNPATENTABLE

A. [GROUND 1] – Claims 1, 3, 4, 7, 8, 10, 12, and 13 Are Anticipated By Aventail (Ex. 1007)

Aventail (Ex. 1007) is a printed publication that was publicly distributed no later than January 31, 1999. Ex. 1005 at ¶¶ 11-36; Ex. 1006 at ¶¶ 11-24. Aventail is prior art to the '135 patent at least under 35 U.S.C. §§ 102(a) and (b). A concise summary of the systems and processes described in Aventail is provided at ¶¶ 18 to 53 of Ex. 1003 and at ¶¶ 37 to 81 of Ex. 1005.

The Aventail publication consists of two documents that cross-reference each other extensively; namely, the Aventail Connect v3.01/v2.51 Administrator's Guide ("Aventail Connect") and the Aventail Extranet Center v3.0 Administrator's Guide ("Aventail Extranet Center"). *See* Ex. 1003 at ¶ 19; *see also* Ex. 1007 at 125-129. The two documents were distributed together with software installation media as part of a single commercial product. *See* Ex. 1005 at ¶¶ 23-36. The two documents describe the configuration and operation of client and server parts of a single Aventail VPN system. *See* Ex. 1003 at ¶ 19; Ex. 1005 at ¶¶ 23-36. The documents together, thus, constitute a single publication, Aventail (Ex. 1007). If the Board determines the two documents do not constitute a single printed publication, the Board should treat Aventail as consisting of the Aventail Connect document, which incorporates by reference specific portions of the Aventail Extranet Center document. *See* Ex. 1005 at ¶ 29.

1. Aventail Anticipates Claim 1

Aventail describes processes that automatically and transparently establish a VPN between a client computer and a remote private network in response to a user specifying a secure destination in a connection request. *See* Ex. 1007 at 11-12, 76-77; *see also* Ex. 1003 at ¶¶ 21, 26, 29, 46. Aventail therefore shows "*[a] method for transparently creating a virtual private network (VPN) between a client computer and a target computer*." *See* Ex. 1003 at ¶¶ 21, 26, 29, 46.

Aventail discloses the step of "*generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer*." In particular, Aventail explains that Aventail Connect, running on a client computer, intercepts each domain name lookup and connection request made by the client computer and evaluates the request. *See* Ex. 1007 at 12-14; *see also* Ex. 1003 at ¶ 29. Furthermore, Aventail describes that "[t]he application does a DNS lookup to convert the hostname to an IP address." Ex. 1007 at 15. In other words, the lookup requests received by Aventail Connect are requests that request an IP address corresponding to a domain name associated with the target computer. Ex. 1003 at ¶¶ 34-35.

Aventail describes a process including a step of "*determining whether the DNS request transmitted in step (1) is requesting access to a secure web site*." *See* Ex. 1003 at ¶¶ 34-36, 42. Aventail explains redirection rules contain domain names or IP addresses associated with destinations requiring secure communications and are used to identify connection requests made by a client computer containing these domain names or IP addresses. *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 38-40. Aventail Connect is configured to evaluate domain name look-up and connection requests locally based on these redirection rules. *See* Ex. 1003 at ¶¶ 37, 41-42.

Aventail describes the step of "*in response to a determination that the DNS request is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer*." *See* Ex. 1003 at ¶¶ 42-46. Aventail shows

that if a domain name or IP address in a DNS request matches a redirection rule, the request will be flagged for special handling by Aventail Connect (e.g., by inserting a false entry ("HOSTENT") in the request). *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 34-35. Then, after the name resolution step, the corresponding connection request will be evaluated – if it contains the false entry or an IP address matching a redirection rule, Aventail Connect is configured to send ("proxy") the request to the proxy server (AES) specified in the redirection rule for that domain name or IP address. *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 43-46. To do this, Aventail Connect opens a connection to the AES and authenticates the user. *See* Ex. 1007 at 16; *see also* Ex. 1003 at ¶¶ 46-47. If authentication is successful, the original request is sent to the server, and communications proceed. *See* Ex. 1007 at 16. Aventail also explains that communications between the client and the private network are automatically encrypted/decrypted. *See* Ex. 1007 at 15-16, 76-77; *see also* Ex. 1003 at ¶¶ 22, 26, 48-49.

Aventail thus anticipates claim 1 as it shows a process including all of the steps specified in that claim.

2. Aventail Anticipates Claim 10

Aventail thus describes a "*system that transparently creates a virtual private network (VPN) between a client computer and a secure target computer*." *See* Ex. 1003 at ¶¶ 21, 26, 29, 46. Aventail describes systems which transparently establish VPNs between a client computer running Aventail Connect and a corporate network via an Aventail ExtraNet

Server ("AES"). *See* Ex. 1007 at 11; *see also* Ex. 1003 at ¶¶ 21, 26, 29, 46. Network traffic between the client and corporate network is automatically encrypted/decrypted. *See* Ex. 1007 at 15-16, 76-77; Ex. 1003 at ¶¶ 22, 26, 48-49.

Aventail shows "*a DNS proxy server that receives a request from the client computer to look up an IP address for a domain name, wherein the DNS proxy server returns the IP address for the requested domain name if it is determined that access to a non-secure web site has been requested, and wherein the DNS proxy server generates a request to create the VPN between the client computer and the secure target computer if it is determined that access to a secure web site has been requested*." *See* Ex. 1003 at ¶¶ 34-35, 42-48. In particular, Aventail shows a client computer running Aventail Connect will intercept and evaluate domain name lookup and connection requests. *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 37, 41-42. Under the broadest reasonable constructions, this is the same technique described in the '135 patent. *See* Ex. 1001 at 38:23-33; *see also* Ex. 1003 at ¶ 32. Aventail also shows the evaluation of a request may be performed by the client computer. *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 34-37, 41-42. In particular, the Aventail Connect client can be configured to intercept and evaluate DNS lookup requests locally and respond in place of a DNS server. *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 33-35, 41-42.

A "DNS Proxy Server" can be on the same or a different computer as the one where the request originates. *See* § III.C.6 *supra*; *see also* Ex. 1003 at ¶ 31. It also can be a

"process" which is performed on a single computer or by several computers working together. *See* § III.C.6 *supra*; Ex. 1003 at ¶ 31. Thus, Aventail Connect can be "a DNS proxy server" within the broadest reasonable construction of that term. *See* § III.C.6 *supra*; Ex. 1003 at ¶ 31.

Aventail describes systems that determine if a connection request contains a domain name or an IP address that matches a redirection rule, and if it does, will establish a VPN between the client computer and the private network specified in the request. *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 42-47. This process involves Aventail Connect intercepting a DNS lookup request sent by a requesting application. *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 34-35. Aventail also shows that if a request contains a domain name or IP address that does not match a redirection rule or an entry in a "local domain resolution" rule, the request is passed through to the operating system of the client computer for handling. *See* Ex. 1007 at 15-16, 76-77; *see also* Ex. 1003 at ¶¶ 35-36.

Aventail describes a system comprising a "*gatekeeper computer that allocates resources for the VPN between the client computer and the secure web computer in response to the request by the DNS proxy server*." The Aventail ExtraNet Server (AES) is a "gatekeeper computer" because it is connected both to a private network and the Internet, and will pass authorized network traffic from one network over to the other. *See* Ex. 1007 at 76-77, 173; *see also* Ex. 1003 at ¶¶ 25, 46-47. The AES receives and evaluates requests from client computers, handles authentication and encryption of data sent between it and the cli-

ent computer, and routes traffic to specified destinations on the private network. *Id.* Because Aventail describes systems having all the elements specified in claim 10 under the broadest reasonable constructions, it anticipates this claim under § 102(b).

3. Aventail Anticipates Claim 13

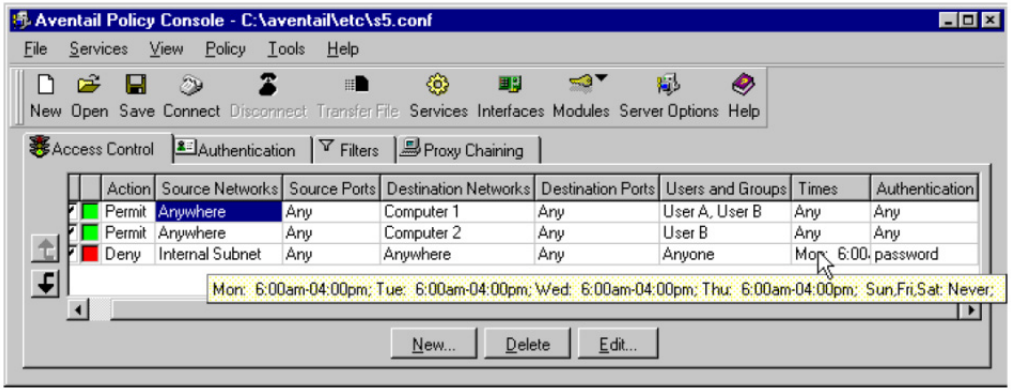
Aventail shows "*A method of establishing communication between one of a plurality of client computers and a central computer that maintains a plurality of authentication tables each corresponding to one of the client computers*…" *See* Ex. 1003 at ¶¶ 20-23, 51-53. Aventail describes systems in which client computers gain access to and communicate with computers on a private network via a gatekeeper computer (the AES). *See* Ex. 1007 at 15-16, 76-77; *see also* Ex. 1003 at ¶¶ 25, 46-47. Aventail shows multiple remote client computers may access corporate network resources. *Id.* The AES authenticates each client computer before establishing a VPN involving that client computer. *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶ 47. The AES can be configured to use a variety of authentication techniques, all of which function to test whether a known user has presented correct credentials. *See id.*

Aventail explains the Aventail ExtraNet Server is configured by defining users and/or groups of users, setting "access control" policies for users and defining "authentication rules" to determine if users are granted access to a network to which the AES is regulating access. *See* Ex. 1007 at 46, 76-77; *see also* Ex. 1003 at ¶¶ 51-53. Also, the AES can be configured to enforce policies that determine which users can remotely gain access to a

protected network, what resources each user will be allowed to access, and other variables. *Id.* The AES will use user credentials and attributes of a client computer to evaluate connection requests. *See* Ex. 1007 at 139; *see also* Ex. 1003 at ¶ 52. The AES stores its settings in configuration files on its local storage, which may take the form of a table. *See* Ex. 1007 at 139; *see also* Ex. 1003 at ¶ 52.

Aventail shows a process including the step of "*in the central computer, receiving from one of the plurality of client computers a request to establish a connection*." *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 34-35. In Aventail, if a connection request is made on a client computer that specifies a domain name or IP address matching a redirection rule, the client computer will attempt to establish a connection with a specified AES. *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 43-46.

Aventail shows a method including the step of "*authenticating, with reference to one of the plurality of authentication tables, that the request received in step (1) is from an authorized client*." *See* Ex. 1007 at 16, 32, 46-62, 139, 156-167; *see also* Ex. 1003 at ¶¶ 47, 51-53. Aventail explains that the AES will determine if a user who has made a connection request is authorized to gain access to network resources using data it maintains about users, groups of users, policies, authentication options and other parameters. *See* Ex. 1007 at 16, 156; *see also* Ex. 1003 at ¶¶ 47, 51. This authentication data may be stored in a table, such as the one shown in the Access Control Tab of the Aventail Policy Console, a screenshot of which is shown below. *See* Ex. 1007at 139; *see also* Ex. 1003 at ¶ 52.



Ex. 1007, p. 139.

Aventail shows a process including the step of "*responsive to a determination that the request is from an authorized client, allocating resources to establish a virtual private link between the client and a second computer*." *See* Ex. 1007 at 15-16, 51; *see also* Ex. 1003 at ¶ 46. Aventail shows that the AES, after determining that a user is authorized and working with Aventail Connect on the client computer, will establish a secure communication channel with the client computer. *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 41, 43-46. The network traffic sent between the client computer and the private network will be encrypted. *See* Ex. 1007 at 15-16, 76-77; *see also* Ex. 1003 at ¶¶ 22, 26, 48-49; § III.C.2 *supra*. Aventail also describes systems that enable a client computer running Aventail Connect to directly communicate with computers (e.g., hosts) on an internal network. *See* § 1 *supra*, above; Ex. 1003 at ¶¶ 48-49.

Aventail shows a process including the step of "*communicating between the authorized client and the second computer using the virtual private link*." *See* Ex. 1003 at ¶¶ 48-49. Aventail explains that once the VPN is established with the client computer, network

traffic will be sent between that client and the involved computer(s) on the private network, and that this traffic will be automatically encrypted. *See* Ex. 1007 at 15-16; Ex. 1003 at ¶¶ 48-49. Aventail anticipates claim 13 because it shows a process with every step recited in claim 13.

4. Aventail Anticipates Claim 3

Aventail shows a process including the step of "*in response to determining that the DNS request in step (2) is not requesting access to a secure target web site, resolving the IP address for the domain name and returning the IP address to the client computer*." *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 34-36. Aventail shows that if a connection request contains a domain name or an IP address that does not match a redirection rule, that request will be passed through to the client operating system "as if Aventail Connect were not running." *See* Ex. 1007 at 15-16, 76-77; *see also* Ex. 1003 at ¶¶ 34-36. Domain names and IP addresses that match a redirection rule that proxies the connection request to the AES trigger VPNs and are "secure" destinations – other domains thus are "non-secure" from the perspective of the Aventail Connect and the AES. *See* Ex. 1003 at ¶¶ 34-36.

5. Aventail Anticipates Claim 4 and 12

Aventail shows a process in which "*prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client computer is authorized to establish a VPN with the target computer and, if not so authorized, returning an error from the DNS request*" pursuant to claim 4. *See* Ex. 1003 at ¶ 41. Aventail describes

methods and systems in which a user that makes a request to access a resource on a private network will be required by the AES to present user credentials before the VPN involving that client computer and the private network is established. *See* Ex. 1003 at ¶¶ 40-41. Aventail explains that the client can be configured to evaluate domain names locally. *See* Ex. 1007 at 15-16, 42-44; *see also* Ex. 1003 at ¶¶ 40-41. If the domain name in a request matches a redirection rule that specifies redirection, the client computer will try to connect to the AES associated with that domain name in the redirection rule. *See* Ex. 1003 at ¶¶ 41-42. To establish a connection to the AES, Aventail Connect must successfully authenticate the client computer before the proxied request or any subsequent data is sent to the AES. *See* Ex. 1003 at ¶¶ 41. If authentication fails, an error will be returned to the calling application. *See* Ex. 1007 at 6, 15-16, 83-86; *see also* Ex. 1003 at ¶¶ 40-41.

Aventail shows a gatekeeper computer that "*determines whether the client computer has sufficient security privileges to create the VPN and, if the client computer lacks sufficient security privileges, rejecting the request to create the VPN*." The AES in this scheme is a "gatekeeper computer." *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 25-26, 46-47. As explained above, the AES requires a client computer to successfully authenticate before a connection request or data will be sent between it and the client computer. *See id.* Also, the AES uses access control rules and filters to determine if a particular user is authorized to access particular resources on a private network. *See id.*

6. Aventail Anticipates Claim 7

Aventail shows "*a gatekeeper computer that allocates VPN resources for communicating between the client computer and the target computer*" which anticipates claim 7. *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 25-26, 46-47. Aventail shows that the AES is a "gatekeeper computer" that authenticates client computers, proxies authorized network traffic onto a private network according to policies it administers, and performs other VPN-related functions. *See id*.; *see also* § 5, *supra*.

7. Aventail Anticipates Claim 8

Aventail shows a process "*wherein step (2) is performed in a DNS proxy server that passes through the request to a DNS server if it is determined in step (3) that access is not being requested to a secure target web site*" which anticipates claim 8. *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 29-31, 33-36. As described above, Aventail Connect acts as a DNS proxy server to the requesting application. Moreover, Aventail shows a connection request containing a domain name that does not match a redirection rule is passed through to the client operating system for handling. *See* Ex. 1007 at 15-16; *see also* Ex. 1003 at ¶¶ 33-36. The native DNS name resolution processes of the client computer act on and resolve the domain name. *See id.*

B. [GROUND 2] – Aventail Connect In View of Aventail Extranet Center Renders Claims 1-10, 12-15 and 18 Obvious

As explained above in §§ A.1 to A.7, *supra*, Aventail anticipates claims 1, 3, 4, 7, 8, 10, 12, and 13. Patent Owner may contend that Aventail does not anticipate those claims because Aventail Connect and Aventail Extranet Center cannot be considered a single doc-

ument. This distinction, if established, would not render these claims patentable. The two documents – Aventail Connect and Aventail Extranet Center – plainly refer to each other and are describing two parts of a single system. A person of ordinary skill in the art would have considered the two documents together. *See* Ex. 1003 at ¶ 19. For example, Aventail Connect states that Aventail Connect is "client component of the Aventail ExtraNet Center." Ex. 1007 at 5. When the teachings of the Aventail Connect document are considered in conjunction with the teachings of the Aventail Extranet Center document, they plainly suggest a system that would have all of the elements and functionality of the methods and systems that are the subject of the claims of the '135 patent. Consequently, for essentially the same reasons presented in §§ A.1 to A.7, *supra*, Aventail Connect in view of Aventail Extranet Center would have rendered obvious claims 1, 3, 4, 7, 8, 10, 12, and 13 of the '135 patent.

C. [GROUND 3] – Aventail In View of RFC 1035 Renders Claim 4 Obvious

Aventail anticipates or renders obvious claim 4. *See* §§ A.5 and B, *supra*. Patent Owner may contend Aventail does not expressly show that an error is returned if a client computer is not authorized to establish a VPN with a target computer (claim 4). This distinction, if established, would not render the claims patentable.

The Aventail systems use DNS servers, which were known in the prior art to perform specific functions in a standardized manner. *See* Ex. 1003 at ¶¶ 54-56. RFC 1035 describes these standardized procedures. *See* Ex. 1017 at 1; *see also* Ex. 1003 at ¶ 55. In-

tegral to this standardized DNS functionality is the ability of a DNS server to return a message containing one of several error codes to a requesting application if it is unable to resolve a supplied domain name. *See id.* These standard error codes include that the request is not authorized (i.e., RCODE 5). *See* Ex. 1003 at ¶¶ 55-56.

A person of ordinary skill would have recognized that the Aventail systems use a proxy server (AES) that requires authentication in order to respond to connection request. *See* Ex. 1003 at ¶¶ 56. That person also would recognize that RCODES in the DNS scheme exist and that RCODES return errors when a DNS server refuses or does not respond, which would occur if authentication failed. *See id.* From these points, a person of ordinary skill in the art would have recognized that the step of having the proxy server or Aventail Connect client return an RCODE to a requesting application if a user failed authentication would have been an obvious design choice given how the DNS scheme functions. *See id.* Consequently, that person would have considered the step of "returning an error code" specified in claim 4 to have been obvious based on Aventail in view of RFC 1035.

D. [GROUND 4] – Claims 1-4, 7, 8, 10, and 12 Are Anticipated by Kiuchi (Ex. 1066)

Kiuchi is a printed publication that was presented at the 1996 Symposium on Network and Distributed Systems Security (SNDSS) on February 22 & 23, 1996, and published by IEEE in the Proceedings of SNDSS 1996. Kiuchi was distributed publicly without restriction no later than February 1996. *See* Ex. 1066. Kiuchi is prior art to the '135 patent at least under § 102(b). Kiuchi is summarized at paragraphs 57-79 of Ex. 1003.

1. Kiuchi Anticipates Claim 1

Kiuchi shows "*[a] method for transparently creating a virtual private network (VPN) between a client computer and a target computer*." *See* Ex. 1003 at ¶ 70. Kiuchi describes a method (termed "C-HTTP") for constructing a closed network over the Internet that allows a user agent (*e.g.*, a web browser) running on a computer in one private network to access private web pages (e.g., HTML pages) stored on an origin server in a different private network. *See* Ex. 1066 at pp. 64, 69. The closed network is created over the Internet using a client-side proxy and a server-side proxy that transparently perform specialized proxy functions for the user agent and origin server. *Id.* at 64-65. The proxies are installed in firewalls between the user agent and the origin server, which are unaware of the proxies. *Id.* The user agent, origin server, and proxies are HTTP/1.0 compatible devices. *Id.* The proxies work in conjunction with a C-HTTP name server on the Internet. *Id.*

Kiuchi describes systems and processes in which a secure connection between a client-side proxy and a server-side proxy (and by extension between the user agent and origin server, which are secured behind the firewalls containing the proxies) automatically is established by the proxy servers and a C-HTTP name server in response to a request specifying a destination in the closed network. *See* Ex. 1003 at ¶¶ 57-59, 70. The proxy servers automatically initiate the secure connection and automatically encrypt any traffic sent over the Internet between the user agent and the origin server without interaction by the user. *Id.*

Kiuchi discloses a process that includes "*generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer*." *See* Ex. 1066 p. 65, § 2.3; *see also* Ex. 1003 at ¶¶ 59-61. Kiuchi shows that a user agent makes an HTTP request to connect to a host that is specified within a URL. *See id.* The client-side proxy receives the request and sends a request to a C-HTTP name server asking to resolve the hostname in the request into an IP address. *See id.*

If the hostname in the URL corresponds to a secure destination and the C-HTTP name server determines the client-side proxy is authorized to make a connection with the server-side proxy, the C-HTTP name server will return an IP address corresponding to the hostname to the client-side proxy. *See* Ex. 1066 p. 65, § 2.3; *see also* Ex. 1003 at ¶¶ 62-63.

Kiuchi describes processes that include the step of "*determining whether the DNS request transmitted in step (1) is requesting access to a secure web site*." *See* Ex. 1066 p. 65, § 2.3; *see also* Ex. 1003 at ¶¶ 61-65. As described above, when the client-side proxy receives the request from the user agent, it sends a request to a C-HTTP name server. *See id.* The C-HTTP name server evaluates the request to determine if the hostname specifies a destination that is part of the closed network and whether the connection between the user agent and the origin server is permitted. *See id.* If the C-HTTP server determines the destination is not part of the closed network, it returns an error code. *See id.* If the client-

side proxy receives an error code, it concludes the request specifies a non-secure destination and sends the hostname to a conventional DNS server. *See id.*

If the C-HTTP name server determines the hostname specifies a secure destination and the connection is permitted, it will return an IP address associated with the secure hostname along with other information. *See id.* The client-side proxy uses the returned IP address to send a request to the server-side proxy to make a connection. *See id.* Thus, the C-HTTP name server and client-side proxy each determine whether the user agent is requesting to connect to a secure destination. *See* Ex. 1003 at ¶¶ 62-63.

Kiuchi shows a process that includes "*in response to a determination that the DNS request is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer*." *See* Ex. 1066, pp. 65-66, § 2.3; *see also* Ex. 1003 at ¶¶ 63, 68-70. Kiuchi shows that if a connection is permitted, the C-HTTP name server initiates the connection by returning an IP address and public key associate with the hostname. *See* Ex. 1066, pp. 65-66, § 2.3; *see also* Ex. 1003 at ¶¶ 62-63, 66. The client-side proxy sends an encrypted connection request to the server-side proxy. *See id.* This is consistent with the '135 patent, which shows an example of automatically initiating a VPN by sending a message requesting to create a VPN. *See id.*; *see* Ex. 1001 at 38:30-33.

If the server-side proxy accepts the connection, it sends to the client-side proxy a message containing a data exchange key. *See* Ex. 1066, pp. 65-66, § 2.3; *see also* Ex. 1003 at ¶¶ 66-69. After the client-side proxy receives the message, a connection is estab-

lished. *See id.* Data is securely transmitted between the user agent and origin server because the proxy servers automatically encrypt any traffic sent between them. *See* Ex. 1066 at p. 65, § 1; *see also* Ex. 1003 at ¶ 65. The connect message the client-side proxy sends to the server-side proxy and the response message the server-side proxy sends to the client-side proxy (both of which are sent without intervention from the user agent) act to initiate the connection. *See* Ex. 1066, pp. 65-66, § 2.3; *see also* Ex. 1003 at ¶¶ 66-69.

2. Kiuchi Anticipates Claim 3

Kiuchi shows a process including the step of "*(4) in response to determining that the DNS request in step (2) is not requesting access to a secure target web site, resolving the IP address for the domain name and returning the IP address to the client computer*." *See* Ex. 1066 p. 65, § 2.3; *see also* Ex. 1003 at ¶¶ 61-64. Kiuchi shows that when the client-side proxy receives an HTTP request, it sends a request to a C-HTTP name server. *See id.* If the destination is not part of the closed network, the C-HTTP name server returns an error code. *See id.* If the client-side proxy receives an error code, it determines the URL specifies a non-secure destination and it sends the hostname in the URL to a conventional DNS server. *See id.* The DNS server will return an IP address, which the client-side proxy uses to establish an ordinary HTTP connection. *See id.*

3. Kiuchi Anticipates Claim 4

Kiuchi shows a process including the step of "*prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client com-*

puter is authorized to establish a VPN with the target computer and, if not so authorized, returning an error from the DNS request." *See* Ex. 1066 p. 65, § 2.3; *see also* Ex. 1003 at ¶¶ 61-64. Kiuchi shows that when the client-side proxy receives an HTTP request from a user agent, it sends a request to a C-HTTP name server. *See id.* The C-HTTP name server authenticates the request and then evaluates it to determine if the connection is permitted. *See* Ex. 1003 at ¶¶ 61-64; Ex. 1066 at pp. 64-65 ("the name server . . . examines whether the client-side proxy is permitted to access to the server-side proxy."). If the C-HTTP name server determines the connection is not permitted, it returns an error code. *See* Ex. 1003 at ¶¶ 61-64.

4. Kiuchi Anticipates Claim 7

Kiuchi shows processes "*wherein step (3) comprises the step of using a gatekeeper computer that allocates VPN resources for communicating between the client computer and the target computer*." *See* Ex. 1003 at ¶ 69. Kiuchi shows that the server-side proxy acts as a gatekeeper computer that allocates resources. *See* Ex. 1003 at ¶ 69. When the client-side proxy receives the request from the user agent, it sends a request to a C-HTTP name server. *See* Ex. 1066, p. 65, § 2.3; *see also* Ex. 1003 at ¶ 62. If the C-HTTP name server determines the connection is permitted, it will return an IP address and public key corresponding to the hostname; otherwise it will return an error code. *See id.* If an IP address and key are returned, the client-side proxy sends an encrypted request to the server-side proxy containing a data exchange key; if an error message is returned the client-side proxy

performs a standard DNS lookup. *See* Ex. 1066, p. 65, § 2.3; *see also* Ex. 1003 at ¶¶ 66-69.

After the server-side proxy receives the request from the client-side proxy, it sends a message to the C-HTTP name server to verify the client-side proxy is part of the closed network. *See id.* If the server-side proxy determines it should accept the connection, it sends a message to the client-side proxy containing a connection identifier and a second data exchange key. *See id.* After the client-side proxy receives the message from the server-side proxy, the connection is established. *See id.* The server-side proxy acts as a gatekeeper by providing the client-side proxy with the connection identifier and the second data exchange key. *See* Ex. 1003 at ¶ 69. This is consistent with the '135 patent specification, which shows the gatekeeper may receive a request from the DNS proxy requesting that a VPN be created. *See* Ex.1001 at 38:30-33.

5. Kiuchi Anticipates Claim 8

Kiuchi shows "*[t]he method of claim 1, wherein step (2) is performed in a DNS proxy server that passes through the request to a DNS server if it is determined in step (3) that access is not being requested to a secure target web site*." *See* Ex. 1066, pp. 65, § 2.3; *see also* Ex. 1003 at ¶¶ 62-65. Kiuchi describes the client-side proxy as a DNS proxy server. *See* Ex. 1003 at ¶ 58. When the client-side proxy receives a request from a user agent, it determines whether the requested hostname in the URL specifies a secure server by sending to a C-HTTP name server a request to resolve the hostname. *See* Ex. 1066, pp. 65, §

2.3; *see also* Ex. 1003 at ¶¶ 62-65. If the C-HTTP name server returns an error code, the client-side proxy determines the URL specifies a non-secure destination. *See id.* The client-side proxy then sends the hostname to a conventional DNS server for resolution. *See id.* This is similar to the '135 patent, under the broadest reasonable construction, where a DNS lookup is performed when access is not being requested to a secure target web site. Ex. 1001 at 38:43-47.

6. Kiuchi Anticipates Claim 10

Kiuchi shows a "*system that transparently creates a virtual private network (VPN) between a client computer and a secure target computer*." *See* Ex. 1003 at ¶ 70. Kiuchi describes systems in which a VPN between a user agent and origin server is automatically and transparently established by proxy servers and a C-HTTP name server. *See* § 1, *supra*. Kiuchi shows that the C-HTTP name server and proxy servers are part of a system of computers. *See* Ex. 1003 at ¶¶ 57-58.

Kiuchi shows a "*gatekeeper computer that allocates resources for the VPN between the client computer and the secure web computer in response to the request by the DNS proxy server*" as specified in claim 10. As explained with respect to claim 7 (see § 4, *supra*), Kiuchi shows that the server-side proxy acts as a gatekeeper that allocates VPN resources.

Kiuchi shows a system including "*a DNS proxy server that receives a request from the client computer to look up an IP address for a domain name, wherein the DNS proxy server returns the IP address for the requested domain if it is determined that the access to*

a non-secure website has been requested, and wherein the DNS proxy server generates a request to create the VPN between the client computer and the secure target computer if it is determined that access to a secure web site has been requested." *See* Ex. 1003 at ¶¶ 58, 60-64, 66. When the client-side proxy receives from the user agent a request to retrieve a resource on an origin server, it sends a request to a C-HTTP name server to resolve a corresponding domain name. *See* Ex. 1066 p. 65, § 2.3; *see also* Ex. 1003 at ¶¶ 59-61. If the C-HTTP name server determines the destination is not part of the closed network, it returns an error code. *See id.* If the client-side proxy receives an error code, it concludes the hostname in the URL specifies a non-secure destination and sends the hostname to a conventional DNS server. *See id* If the C-HTTP name server determines the hostname specifies a secure destination, it returns an IP address and other information. *See id.* Thus, where a user agent requests to connect to a destination in the closed network, the C-HTTP name server and client-side proxy act as proxy servers, acting in place of a conventional DNS server. *See id.* But where the user agent requests to connect to a non-secure server, the hostname in the connection request will be resolved by a conventional DNS. *See id*

7. Kiuchi Anticipates Claim 12

Kiuchi shows a process comprising "*wherein the gakekeeper computer determines whether the client computer has sufficient security privileges to create the VPN, and, if the client computer lacks sufficient security privileges, rejecting the request to create the VPN*." *See* Ex. 1003 at ¶ 69. As explained above with respect to claim 7 (see § 4, *supra*), Kiuchi

shows the server-side proxy acts as a gatekeeper that allocates VPN resources. If the server-side proxy determines a requested connection is not permitted, it does not accept the client-side proxy's connection request. *See* Ex. 1003 at ¶¶ 66-67.

E. [GROUND 5] – Kiuchi In View of RFC 1034 Renders Claim 8 Obvious

Kiuchi explains its systems enable users to securely access resources in various private networks by establishing a closed network over the Internet. *See* Ex. 1066 at p. 64, § 21; Ex. 1003 at ¶ 57-58. Kiuchi defines three specialized parts for the system: the client-side proxy, server-side proxy, and C-HTTP name server. *See id.* While Kiuchi describes the client-side proxy makes a conventional DNS lookup request, a person of ordinary skill would have recognized that the DNS lookup step could be integrated into the C-HTTP name server based on the guidance in RFC 1034 (Ex. 1016), which describes the functional requirements of DNS name servers. *See* Ex. 1003 at ¶¶ 73-74. Such a change would have been an obvious design choice. *Id.*

Notably, the C-HTTP name server already determines whether a DNS request is requesting to access a secure web site. *See* Ex. 1066 at 65, § 2.3(2); *see also* Ex. 1003 at ¶ 74. Rather than returning an error code to the client-side proxy when the DNS request does not specify a secure web site, it would have been an obvious design choice for the C-HTTP name server to pass the domain name to a conventional DNS server for resolution, or to perform a standard DNS lookup, since the C-HTTP server already includes name service functionality. *See* Ex. 1003 at ¶ 74. Such a configuration, which places a DNS proxy server

function in a modified C-HTTP name server (similar to placement of the DNS proxy server of the '135 patent in the DNS server – *see* Ex.1001 at FIG. 26), is merely a rearrangement of existing functions within the C-HTTP system. *See* Ex. 1003 at ¶¶ 74-76. For example, a C-HTTP name service response containing an IP address without a public key and nonce values (*e.g.*, using values of zero or other convention for those fields, or modifying the protocol to use a flag in the response to indicate those values are not provided) could indicate that the response specifies a conventional web site and hence that no VPN is needed. *See* Ex. 1003 at ¶¶ 76-77. The motivation for modifying Kiuchi in this way would have been to streamline the system's operation, *e.g.*, instead of the C-HTTP name server sending an error code to the client-proxy which would then initiate a DNS inquiry, the change simplifies the process by having the C-HTTP name server initiate the request to the conventional DNS server. *See* Ex. 1003 at ¶¶ 78-79.

Kiuchi anticipates claim 8. *See* §§ V.D.2 and V.D.5, *supra*. However, Patent Owner may contend Kiuchi does not show a DNS proxy server per claim 8. This distinction, if established, would not render claim 8 patentable. As described above, it would have been an obvious modification of the Kiuchi C-HTTP system to configure the C-HTTP name server to resolve non-secure addresses as well. If the C-HTTP name server received a request to resolve a hostname that was not part of the closed network, it would forward the request to an ordinary DNS server. *See* Ex. 1003 at ¶¶ 76-77. Thus, claim 8 would have been obvious to a person of ordinary skill based on Kiuchi in view of that person's general knowledge.

VI. REDUNDACY

In this petition, Petitioner has presented only a limited number of grounds, yet in doing so, has demonstrated how various teachings address the claims divergently. Indeed, Aventail expressly describes an authentication table (shown by the Access Control Tab of the Aventail Policy Console), as required by claim 13. Ex. 1007 at 139. Moreover, Kiuchi expressly describes two proxy servers (i.e., the client-side and server-side proxies), and is a self-authenticating article with a clear statutory basis as prior art. Ex. 1066 at 69, § 5.

The limited grounds presented in these petitions do not impede "the just, speedy, and inexpensive resolution of [this] proceeding," as required by 37 C.F.R. § 42.1(b). As Petitioner has already limited its petitions to just a few grounds, Petitioner respectfully requests that the Board institute rejections on all grounds presented in these two petitions to avoid prejudicing Petitioner. However, to the extent the Board institutes fewer than the limited number of presented grounds, Petitioner requests that the Board institute at least the Kiuchi-based grounds of rejection for independent claims 1 and 10 and their dependent claims and the Aventail-based grounds of rejection for independent claim 13.

VII. CONCLUSION

The cited prior art references identified in this Petition contain pertinent technological teachings (both cited and uncited), either explicitly or inherently disclosed, which were not previously considered in the manner presented herein, or relied upon on the record during original examination of the '135 patent. In sum, these references provide new, non-

cumulative technological teachings which indicate a reasonable likelihood of success as to Petitioner's assertion that the Challenged Claims of the '135 patent are not patentable pursuant to the grounds presented in this Petition. Accordingly, Petitioner respectfully requests institution of an IPR for those claims of the '135 patent for each of the grounds presented herein.

Respectfully submitted,

Dated: 3/31/14

/W. Karl Renner/

W. Karl Renner, Reg. No. 41,265
Fish & Richardson P.C.
P.O. Box 1022
Minneapolis, MN 55440-1022
T: 202-626-6447
F: 202-783-2331

Dated: 3/31/14

/Kevin E. Greene/

Kevin E. Greene, Reg. No. 46,031
Fish & Richardson P.C.
P.O. Box 1022
Minneapolis, MN 55440-1022
T: 202-626-6376
F: 202-783-2331

(Trial No. _____)

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on March 31, 2014, a complete and entire copy of this Petition for *Inter Partes* Review, Motion for Joinder, and all supporting exhibits were provided via FedEx, to the Patent Owner by serving the correspondence address of record as follows:

Finnegan, Henderson, Farabow
Garrett & Dunner LLP
901 New York Avenue, NW
Washington, DC 20001

/Edward G. Faeth/

Edward G. Faeth
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(202) 626-6420