

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:

Derry SHRIBMAN *et al.*

Serial No.: TBD

Filed: Herewith

For:

Ex parte reexamination of
claims 1-29 of U.S. Patent
No. 10,469,614

Confirmation No.: TBD

Group Art Unit: TBD

Examiner: TBD

Atty Docket No.:

2042-03-614-EPR

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**REQUEST FOR EX PARTE REEXAMINATION OF CLAIMS 1-29 OF U.S.
PATENT NO. 10,469,614**

Sir or Madam:

Pursuant to 35 U.S.C. §§ 302-305 and 37 C.F.R. § 1.510, Ronald Abramson ("Requester") requests reexamination of claims 1-29 of U.S. Patent No. 10,469,614 (the '614 patent), entitled "System and method for improving Internet communication by using intermediate nodes." The '614 patent issued on November 5, 2019, from U.S. Patent Application Ser. No. 16/214,433 (the '433 application), filed December 10, 2018. A copy of the '614 patent is attached to this Request as Ex. 1.

Contents

1 INTRODUCTION	1
2 REQUIREMENTS FOR <i>EX PARTE</i> REEXAMINATION UNDER 37 C.F.R. § 1.510, AND RELATED DISCLOSURES	5
2.1 Statement Pointing Out Each Substantial New Question of Patentability Based on Prior Art Patents and Printed Publications (37 C.F.R. § 1.510(b)(1))	5
2.2 Identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited prior art (37 C.F.R. § 1.510(b)(2))	5
2.3 A copy of every patent or printed publication relied upon or referred to in paragraph (b)(1) and (2) of 37 C.F.R. § 1.510 (37 C.F.R. § 1.510(3))	5
2.4 A copy of the entire patent including the front face, drawings, and specification/claims (in double column format) for which reexamination is requested, and a copy of any disclaimer, certificate of correction, or reexamination certificate issued in the patent. (37 C.F.R. § 1.510(b)(4))	6
2.5 A certification that a copy of the request filed by a person other than the patent owner has been served in its entirety on the patent owner at the address as provided for in § 1.33(c). (37 C.F.R. § 1.510(b)(5))	6
2.6 A certification by the third party requester that the statutory estoppel provisions of 35 U.S.C. 315(e)(1) or 35 U.S.C. 325(e)(1) do not prohibit the requester from filing the <i>ex parte</i> reexamination request. (37 C.F.R. § 1.510(b)(6))	7

2.7	Payment of Fees (37 CFR § 1.510(a))	7
2.8	Disclosure of Related Proceedings	7
3	REVIEW OF THE '614 PATENT, ITS ORIGINAL PROSECUTION, AND CLAIMS	12
3.1	Specification of the '614 Patent	12
3.2	Overview of the '614 Patent Claims	21
3.3	Correspondence of Claims to the '614 Specification—Mapping the '614 Patent to Itself	24
3.4	Priority Date	27
3.5	Prosecution History of the '614 Patent, and Reasons for Al- lowance	28
3.6	Claim Construction	31
4	OVERVIEW OF THE SUBMITTED PRIOR ART	39
4.1	Shribman '733 publication (Ex. 6)	39
4.2	Liu (Ex. 29)	41
4.3	Sigurdsson (Ex. 7)	41
4.4	Chauhan (Ex. 8)	42
4.5	Bhatia (Ex. 17)	42
4.6	Ebata (Ex. 23)	42
4.7	Mithyantha (Ex. 10)	42
4.8	MorphMix (Ex. 11)	44
4.9	RFCs 2616, 791, and 793 (Exs. 12, 22, and 28)	44
4.10	Standard Practices for Application Startup Configuration . . .	45
4.11	Background Prior Art	47
4.12	Applicant Admitted Prior Art (AAPA)	49

5 SUMMARY OF SNQs/PROPOSED REJECTIONS AND WHY THEY RAISE SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY	50
5.1 SNQ I—Grounds based primarily on the Shribman '733 publication	50
5.2 SNQ II—Grounds based primarily on Mithyantha	54
5.3 SNQ III—Grounds based primarily on MorphMix	56
6 PERTINENCE AND MANNER OF APPLYING THE PRIOR ART	57
6.1 Legal Standards	57
6.2 Level of Skill in the Art	62
6.3 Analogous Nature of The Cited Prior Art	63
7 SNQ I: ANTICIPATION AND/OR OBVIOUSNESS GROUNDS AS TO ALL CLAIMS, BASED ON THE SHRIBMAN '733 PUBLICATION	70
7.1 SNQ Ia/Anticipation of Claims 1, 3-5, 7-9, 13, 17, 25-26, and 29 by the Shribman '733 Publication	75
7.2 SNQ Ib: Obviousness of Claims 1-5, 7-9, 13, 17, 25-26, and 29 over the Shribman '733 publication in view of Liu	93
7.3 SNQ Ic: Obviousness of Claims 2-6, 8-10, 14-27, and 29 over the Shribman '733 publication in view of Sigurdsson and/or Chauhan	101
7.4 SNQ Id: Obviousness of Claims 2-6, 8-10, 14-27, and 29 over the Shribman '733 publication in view of Liu and in further view of Sigurdsson and/or Chauhan	116
7.5 SNQ Ie: Obviousness of Claims 11-12 over the Shribman '733 Publication in view of Bhatia	117
7.6 SNQ If: Obviousness of Claims 11-12 over the Shribman '733 Publication in view of Liu and in further view of Bhatia	118

7.7	SNQ Ig: Obviousness of Claim 28 over the Shribman '733 publication in view of Ebata	119
7.8	SNQ Ih: Obviousness of Claim 28 over the Shribman '733 publication in view of Liu and in further view of Ebata	121
8	SNQ II: (a) ANTICIPATION OF CLAIMS 1-2, 4-12, 15-23, 25-26, AND 29 BY MITHYANTHA AND (b) OBVIOUSNESS OF CLAIMS 1-2, 4-12, 15-26, AND 28-29 OVER MITHYANTHA IN VIEW OF INTERNET STANDARDS AND GENERAL KNOWLEDGE OF A POSITA	121
8.1	SNQ IIa (§ 102)/Anticipation of Claims 1-2, 4-12, 15-23, 25-26, and 29 by Mithyantha	124
8.2	SNQ IIb (§ 103)/Obviousness of claims 1-2, 4-12, 15-26, and 28-29 over Mithyantha in View of Internet Standards, Standard Practices for Application Startup Configuration, and General Knowledge of a POSITA	150
9	SNQ III: OBVIOUSNESS OF CLAIMS 1-2, 4-5, 7-10, 13, 17-26, AND 29 OVER MORPHMIX IN VIEW OF STANDARD PRACTICES FOR APPLICATION STARTUP CONFIGURATION AND GENERAL KNOWLEDGE OF A POSITA	161
9.1	SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA/Claim 1	163
9.2	SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claim 2	175

9.3 SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claim 4	176
9.4 SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claim 5	176
9.5 SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claim 7	177
9.6 SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claim 8	177
9.7 SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claims 9-10	178
9.8 SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claim 13	179
9.9 SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claim 17	179
9.10 SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claims 18-24	180
9.11 SNQ III (§ 103 Morphmix + Standard Practice for Application Startup Configuration and General Knowledge of a POSITA)/Claims 25-26	183

9.12 SNQ III (§ 103 Morphmix + Standard Practice for Application

Startup Configuration and General Knowledge of a POSITA)/Claim

29 184

10 CONCLUSION

185

EXHIBIT LIST

1	U.S. Patent No. 10,469,614 to Shribman <i>et al.</i>
2	Prosecution History of the '614 patent, s/n 16/214,433
3	Expert Declaration of Keith J. Teruya
4	CV of Keith J. Teruya
5	U.S. Patent Provisional Application No. 61/870,815 (Provisional of '614 family)
6	Shribman '733 Publication, U.S. Patent Pub. No. 2011/0087733 A1
7	Sigurdsson <i>et al.</i> , U.S. Patent Pub. No. 2007/0174246 A1
8	Chauhan <i>et al.</i> , U.S. Patent Pub. No. 2010/0262650 A1
9	Jackowski <i>et al.</i> , U.S. Patent Pub. No. 2013/0304796 A1
10	Mithyantha, U.S. Patent No. 8,972,602
11	Marc Rennhard, MorphMix - A Peer-to-Peer-based System for Anonymous Internet Access (Doctoral Thesis 2004)
12	Roy T. Fielding <i>et al.</i> , Hypertext Transfer Protocol – HTTP/1.1 (RFC 2616) (1999)
13	Duane Wessels, Squid: The Definitive Guide, (Tatiana A. Diaz ed., 1st ed. 2004)
14	Ari Luotonen, Web Proxy Servers (1998)
15	Claim Construction Opinion and Order, <i>Luminati Networks Ltd. v. Teso LT, UAB et al.</i> , No. 2:19-cv-00395-JRG (E.D. Tex.), D.I. 191 (Dec. 7, 2020)
16	Dorso <i>et al.</i> , U.S. Patent Pub. No. 2011/0066924 A1
17	Bhatia <i>et al.</i> , U.S. Patent Pub. No. 2013/0171964 A1
18	Comparison of Claim 1 as originally filed and as issued
19	Doc-to-Doc comparison of Chauhan and Mithyantha specifications
20	Doc-to-Doc comparison of Jackowski and Mithyantha specifications
21	Printed publication support for Morphmix
22	Internet Protocol (RFC 791) (Jon Postel ed., 1981)
23	Ebata <i>et al.</i> , U.S. Patent No. 6,513,061
24	Greg Shultz, "Windows Vista's Task Manager: The harder-to-detect changes," TechRepublic (Feb. 2007), <i>available at</i> https://www.techrepublic.com/article/windows-vistas-task-manager-the-harder-to-detect-changes/

Exhibit List (Continued)	
25	Gavin Gear, “Windows 8 Task Manager In-Depth,” Windows (June 2013), <i>available at</i> https://blogs.windows.com/windowsexperience/2013/06/06/windows-8-task-manager-in-depth/
26	Scott Lowe, “Use Resource Monitor to monitor network performance,” TechRepublic (July 2011), <i>available at</i> https://www.techrepublic.com/blog/the-enterprise-cloud/use-resource-monitor-to-monitor-network-performance/
27	Erich Gamma <i>et al.</i> , Design Patterns: Elements of Reusable Object-Oriented Software (1st ed. 1994)
28	Transmission Control Protocol (RFC 793) (Jon Postel ed., 1981)
29	Liu, U.S. Patent Pub. No. 2010/0082513 A1
30	Supplemental Claim Construction Opinion and Order, <i>Luminati Networks Ltd. v. Teso LT, UAB et al.</i> , No. 2:19-cv-00395-JRG (E.D. Tex.), D.I. 453 (Aug. 6, 2021)
31	“Glossary of Terms for Device Independence,” W3C (Jan. 2005) <i>available at</i> https://www.w3.org/TR/di-gloss/#ref-wca-terms
32	Transcript of Pretrial Conference, <i>Luminati Networks Ltd. v. Teso LT, UAB et al.</i> , No. 2:19-cv-00395-JRG (E.D. Tex.) (Aug. 31-Sept. 1, 2021)
33	“Geolocation API Specification,” W3C (Oct. 24, 2013) <i>available at</i> https://www.w3.org/TR/2013/REC-geolocation-API-20131024/
34	Yong Wang <i>et al.</i> , <i>Towards Street-Level Client-Independent IP Geolocation</i> (2011)
35	L.J. Fogel <i>et al.</i> , “Modeling the Human Operator with Finite-State Machines,” NASA Contractor Report (NASA CR-1112) (July 1968)
36	IPR2021-00458, Paper 11 at 19 (Institution Decision, concerning Patent Owner’s Patent No. 9,241,044)
37	IPR2021-00465, Paper 11 at 14-15 (Institution Decision, concerning Patent Owner’s Patent No. 9,742,866)
38	Materials considered by Keith J. Teruya

1. INTRODUCTION

Requester respectfully requests *ex parte* reexamination of claims 1-29 (the “Challenged Claims”) of U.S. Patent No. 10,469,614 (the “’614 patent”) (Ex. 1), in light of substantial new questions of patentability (SNQs) as presented herein. This request further is supported by the accompanying expert declaration of Keith J. Teruya (Ex. 3), and the other documents identified in the Exhibit List above. Due to the earliest claimed priority date of this patent being after March 16, 2013, the requested reexamination is subject to the first inventor to file (FITF) provisions of the AIA.

* * * * *

The ’614 patent concerns the common process of Internet content retrieval through an intermediate device (*i.e.*, “proxy”):

user computer (a) <==> proxy (b) <==> web server (c)

Proxies have been used since nearly the beginning of the Internet for a variety of purposes. These purposes include:

- on the client side, to centralize and regulate employee access to the Internet in an enterprise network, by locating a proxy in the enterprise firewall to serve as a managed gateway for enterprise workstations wishing to access the Internet
- on the server side, to transparently load-balance incoming content requests to a server by setting up a plurality proxies to relay incoming requests to appropriate back-end server resources

- in a “content delivery network,” to pre-cache content to a plurality of “edge” locations likely to be closer to users (in terms of Internet “hops”), in order to speed up content delivery

Some of these legacy uses of proxies are summarized in the '614 patent itself (*see, e.g.*, Ex. 1 at 27:14-43, 42:48-43:12).

Other well-known uses of proxies are documented in standard texts, such as the book, “Squid,” by Wessels (2004) (*see, e.g.*, Ex. 13 at 1-2, 86) documenting an open source proxy server by that name), and the earlier work on Web Proxies, by Luotonen (1998) (*see, e.g.*, Ex. 14 at 147-48). (For further information of a background nature with regard to proxies see the accompanying expert declaration of Keith J. Teruya, Ex. 3 ¶¶ 34, 102-05).

The above-identified references, each examined in further depth herein, reflect that the use of proxies to intermediate Internet content retrieval, for any number of reasons, has been very common and well known, for decades.

Moreover, the practice of selecting a particular proxy from a *group* of available proxy devices has also been very widely practiced over the same period. *See, e.g.*, Squid, Ex. 13, Ch. 10 (“Talking to Other Squids”), at 152; Luotonen, Ex. 14 at 116 (“determin[ing] which one of [a plurality of] proxies should be used to retrieve [specified content]”).

What the '614 patent claims, over this baseline of background prior art, is simply the following: in a network with multiple proxies, providing a simple management overlay that keeps track of which proxies are in an available state at any given time to perform web content retrieval tasks, so as not to assign a device that is overburdened or unavailable.

In other words, the sum and substance of claim 1 is a combination of (1) conventional proxy content retrieval functionality, and (2) assigning content retrieval tasks to the proxies, based on their state of availability.¹

The fact is, however, that selecting among proxies based on their availability was *also* well known. In fact, there was a prior patent application by the same inventive entity—the **Shribman '733 publication**, Ex. 6, U.S. Patent Pub. No. 2011/0087733 A1, published two years before the filing of the 2013 provisional application that led to the '614 patent.² The Shribman '733 publication is strikingly similar in its architecture to the disclosure of the '614 patent, and also discloses a process of proxying and determining availability of proxy devices, with substantially the same features and *in the same combination* as is claimed in the '614 patent.

As addressed in detail herein, the Shribman '733 publication discloses, in combination, *both* tracking the status of content retrieval devices (which also serve as clients) to determine their availability, *and* web content proxy retrieval by those devices, from distinct web servers, as claimed in the '614 patent.

¹ As discussed in greater detail below, the prosecution history of the '614 patent bears out that claim 1 recites nothing more than the proxy management overlay and its use. Claim 1 as issued resulted from the amalgamation of original claim 1, describing the overlay, and original claim 29, reciting the additional step consisting simply of conventional proxied web content retrieval. The combination of these features, presented by way of an amendment well into prosecution (Ex. 2 at 118) became issued claim 1.

² As discussed in further detail herein, the Patent Owner did disclose the Shribman '733 publication during the prosecution of the '614 patent. However, the Shribman '733 publication was never discussed by the applicant or the Examiner on the record, or applied in any action, either by itself or in any combination, and thus properly underpins the SNQ discussed in greater detail below.

Furthermore, additional dependent claims, which add further details to claim 1, are obvious over the Shribman '733 publication in view of prior art that discloses well-known modifications to content retrieval methods that are readily and obviously combinable with claim 1.

Moreover, wholly separate and apart from the Shribman '733 publication, additional and distinct prior art, which was never before the Examiner, independently leads to the same result. In particular, neither of **Mithyantha** (Ex. 10, U.S. Patent No. 8,972,602) nor **Morphmix** (Ex. 11, published 2004 Swiss doctoral thesis), discussed herein, was before the Examiner during original prosecution. Each of these additional references, independently, fully disclose and/or render obvious *both* the proxying *and* monitoring/management aspects of the '614 patent, thereby raising *further* SNQs no less significant than those raised by the Shribman '733 publication.

In sum, taking a known prior art proxied content retrieval task and combining it with a process to make a known prior art determination of the availability of the proxy devices, did not merit a patent in 2013. Like deployments already existed, both with these individual features, and in the claimed combination, in the '614 inventors' previously published work, as well as in other available then-available references, as cited herein.

Requester submits that had the original Examiner had before him and considered the art and combinations thereof presented herein, the '614 patent would not have issued.

2. REQUIREMENTS FOR EX PARTE REEXAMINATION UNDER 37 C.F.R. § 1.510, AND RELATED DISCLOSURES

2.1. Statement Pointing Out Each Substantial New Question of Patentability Based on Prior Art Patents and Printed Publications (37 C.F.R. § 1.510(b)(1))

Requester raises a number of SNQs, based on identical disclosures not heretofore considered as well as analogous references or combinations of references that were not before the Examiner during original prosecution, which anticipate or render obvious each of the claims challenged herein.

Section 5 below (beginning at page 50) addresses the reasons why each of these grounds includes substantial new questions over what was considered in reexamination.

Sections 7-9 below (at pages 70-161) then set forth in detail the substance of each asserted SNQ.

2.2. Identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited prior art (37 C.F.R. § 1.510(b)(2))

The claims for which reexamination is requested are 1-29. A detailed explanation of the pertinency and manner of applying the cited prior art to those claims is set forth in detail in Sections 6 and Sections 7-9 below.

2.3. A copy of every patent or printed publication relied upon or referred to in paragraph (b)(1) and (2) of 37 C.F.R. § 1.510 (37 C.F.R. § 1.510(3))

Pursuant to 37 C.F.R. § 1.510(b)(3), copies of the prior art patents and printed publications that support the proposed rejections are attached to this request. A complete list of these items appears following the Table of Contents above. The prior art patent and printed publications are also

identified in the Information Disclosure Statement on Form PTO/SB/08a filed herewith. All cited references are in English.

2.4. A copy of the entire patent including the front face, drawings, and specification/claims (in double column format) for which reexamination is requested, and a copy of any disclaimer, certificate of correction, or reexamination certificate issued in the patent. (37 C.F.R. § 1.510(b)(4))

Exhibit 1 is a complete copy of the '614 patent as issued by the USPTO. Requester is not aware of any certificate of correction, disclaimer, or reexamination certificate for the '614 patent. To Requester's knowledge, the '614 patent has not expired.

2.5. A certification that a copy of the request filed by a person other than the patent owner has been served in its entirety on the patent owner at the address as provided for in § 1.33(c). (37 C.F.R. § 1.510(b)(5))

The undersigned certifies that a complete and entire copy of this Request for *Ex Parte* Reexamination, together with all supporting documents, has been provided to the Patent Owner by serving the attorney of record at the U.S. Patent and Trademark Office for the '614 Patent as set forth in 37 C.F.R. § 1.33(c):

May Patents Ltd. c/o Dorit Shem-Tov
P.O.B. 7230
Ramat-Gan 5217102
ISRAEL

(PAIR Correspondence Address for U.S. Patent No. 10,469,614)

2.6. A certification by the third party requester that the statutory estoppel provisions of 35 U.S.C. 315(e)(1) or 35 U.S.C. 325(e)(1) do not prohibit the requester from filing the *ex parte* reexamination request. (37 C.F.R. § 1.510(b)(6))

Requester certifies that the statutory estoppel provisions of 35 U.S.C. § 315(e)(1) or 35 U.S.C. § 325(e)(1) do not prohibit Requester or the real party in interest on behalf of which this Request is being filed from filing this *ex parte* Request.

2.7. Payment of Fees (37 CFR § 1.510(a))

The requisite fees under 37 CFR § 1.510(a) are being paid through the undersigned's Deposit Account or via credit card and the USPTO's EFS processing system. The Office is authorized to charge Deposit Account No. 603258 for the fees set forth in 37 C.F.R. § 1.20(c)(1) for reexamination.

2.8. Disclosure of Related Proceedings

The following listed pending litigation, PTAB proceedings, and pending U.S. patent applications concern patents and patent applications claiming the benefit of the '614 patent's underlying provisional application (61/870,815) ("614 Family"), or concern an earlier co-owned patent family by the same inventive entity ("815 Family"), which does not share common priority but presents issues of claim construction and validity that overlap with those raised by the '614 Family.

Because the referenced litigation proceedings have not yet resulted in a final holding of invalidity as to any claims of the '614 patent, they are not controlling in this reexamination. See MPEP § 2242. Moreover, evaluation of the existence of a substantial new question of patentability is to be

undertaken “independently” of any decision of “validity” in a judicial proceeding. *Id.* (citing *In re Swanson*, 540 F.3d 1368, 1378 (Fed. Cir. 2008)). Nevertheless, the following is presented in the interest of full disclosure.

Matter	Subject Matter	Status
<i>Luminati Networks Ltd. v. BI Science (2009) Ltd.</i> , No. 21-1664 (Fed. Cir.)	Appeal	Pending
<i>Luminati Networks Ltd. v. BI Science (2009) Ltd.</i> , No. 21-1667 (Fed. Cir.)	Appeal	Pending
<i>Luminati Networks Ltd. v. BI Science Inc.</i> , No. 20-2181 (Fed. Cir.)	Appeal	Pending
<i>Bright Data Ltd. v. BI Science (2009) Ltd.</i> , No. 20-2118 (Fed. Cir.)	Appeal	Pending
<i>Bright Data Ltd. v. NetNut Ltd.</i> , No. 2-21-cv-00225 (E.D. Tx.)	Patent Nos. 10,257,319 and 10,484,510	Pending
<i>Teso LT et al. v. Bright Data Ltd. and EMK Capital LLP</i> , No. 2-20-cv-00073 (E.D. Tx.)	Patent Nos. 9,241,044, 9,742,866, 10,469,614 , 10,484,510 and 10,257,319	Dismissed (settled)
<i>Luminati Networks Ltd. f/k/a Hola Networks Ltd. v. NetNut Ltd.</i> , No. 2-20-cv-00188 (E.D. Tx.)	Patent Nos. 10,484,511 and 10,637,968	Pending
<i>Luminati Networks Ltd. v. Tefincom SA d/b/a NordVPN</i> , No. 2-19-cv-00414 (E.D. Tx.)	Patent Nos. 10,257,319; 10,469,614 ; 10,484,510; 10,484,511; and 10,637,968	Pending

<i>Luminati Networks Ltd. v. Teso LT, UAB a/k/a UAB Teso LT et al.</i> , No. 2-19-cv-00395 (E.D. Tx.)	Patent Nos. 10,257,319; 10,469,614 ; and 10,484,510	Pending
<i>Bright Data Ltd. v. code200, UAB et al.</i> , No. 2-19-cv-00396 (E.D. Tx.)	Patent Nos. 10,484,511 and 10,637,968	Pending
<i>Luminati Networks Ltd. v. BI Science (2009) Ltd.</i> , No. 2-19-cv-00397 (E.D. Tx.)	Patent Nos. 10,257,319; 10,469,614 ; 10,484,510; and 10,484,511	Pending
<i>Luminati Networks Ltd. v. BI Science (2009) Ltd. a/k/a BIScience Inc.</i> , No. 2-19-cv-00352 (E.D. Tx.)	Patent No. 10,410,244	Pending
<i>Luminati Networks Ltd. v. IP Ninja Ltd.</i> , No. 2-19-cv-00196 (E.D. Tx.)	Patent Nos. 9,241,044 and 9,742,866	Pending
<i>Luminati Networks Ltd. v. BI-Science Ltd. a/k/a BIScience Inc.</i> , No. 2-18-cv-00483 (E.D. Tx.)	Patent Nos. 9,241,044 and 9,742,866	Pending
<i>Luminati Networks Ltd. v. UAB Tesonet</i> , No. 2-18-cv-00299 (E.D. Tx.)	Patent Nos. 9,241,044 and 9,742,866	Pending
<i>Luminati Networks Ltd. v. UAB Tesonet</i> , No. 2-18-cv-00299 (E.D. Tex.)	Patent Nos. 9,241,044 and 9,742,866	Pending

2.8.1. PTAB Proceedings

Matter	Subject Matter
<i>Code200, UAB et al v. Luminati Networks Ltd. f/k/a Hola Networks Ltd.</i> , IPR2020-01266 (Petition denied)	Patent No. 10,257,319

<i>NetNut Ltd. v. Bright Data Ltd. f/k/a Luminati Networks Ltd.</i> , IPR2021-00465 (Petition instituted)	Patent No. 9,742,866
<i>NetNut Ltd. v. Bright Data Ltd. f/k/a Luminati Networks Ltd.</i> , IPR2021-00458 (Petition instituted)	Patent No. 9,241,044
<i>Code200, UAB et al v. Luminati Networks Ltd. f/k/a Hola Networks Ltd.</i> , IPR2020-01358 (Petition denied)	Patent No. 10,484,510
<i>Code200, UAB et al v. Luminati Networks Ltd. f/k/a Hola Networks Ltd.</i> , IPR2020-01506 (Petition denied)	Patent No. 10,469,614
<i>Code200, UAB et al v. Luminati Networks Ltd. f/k/a Hola Networks Ltd.</i> , IPR2021-00249 (Petition denied)	Patent No. 10,637,968
<i>BI Science (2009) Ltd. a/k/a BIScience Inc. v. Luminati Networks Ltd.</i> , IPR2020-00166 (Terminated prior to institution decision)	Patent No. 9,241,044
<i>BI Science (2009) Ltd. a/k/a BIScience Inc. v. Luminati Networks Ltd.</i> , IPR2020-00167 (Terminated prior to institution decision)	Patent No. 9,742,866
<i>Teso LT, UAB f/k/a UAB Tesonet et al v. Luminati Networks Ltd. f/k/a Hola Networks Ltd.</i> , IPR2021-00122 (Petition denied)	Patent No. 10,484,511

2.8.2. Other Potentially Relevant Patents, Patent Applications, and Proceedings

In the following, the "'624 Family" refers to patents claiming priority to provisional application no. 61/249,624, while the "'815 Family" refers to patents claiming priority to provisional application no. 61/870,815.

App. No.	Status/Issued As	Related To
12/836,059	U.S. Pat. No. 8,560,604	'624 Family
14/025,109	U.S. Pat. No. 10,069,936	'624 Family
14/468,836	U.S. Pat. No. 9,241,044	'815 Family
14/930,894	U.S. Pat. No. 9,742,866	'815 Family
15/663,762	U.S. Pat. No. 10,277,711	'815 Family

15/957,942	U.S. Pat. No. 10,313,484	'624 Family
15/957,945	U.S. Pat. No. 10,257,319	'624 Family
15/957,950	U.S. Pat. No. 10,225,374	'624 Family
16/031,636	U.S. Pat. No. 10,616,375	'624 Family
16/140,749	U.S. Pat. No. 10,652,357	'815 Family
16/140,785	U.S. Pat. No. 10,659,562	'815 Family
16/214,451	U.S. Pat. No. 10,440,146	'815 Family
16/214,476	U.S. Pat. No. 10,652,358	'815 Family
16/214,496	U.S. Pat. No. 10,721,325	'815 Family
16/278,104	U.S. Pat. No. 10,523,788	'624 Family
16/278,105	U.S. Pat. No. 10,469,628	'624 Family
16/278,106	U.S. Pat. No. 10,491,712	'624 Family
16/278,107	U.S. Pat. No. 10,484,510	'624 Family
16/278,109	U.S. Pat. No. 10,484,511	'624 Family
16/292,363	U.S. Pat. No. 10,469,615	'815 Family
16/292,382	U.S. Pat. No. 10,447,809	'815 Family
16/292,364	U.S. Pat. No. 10,924,580	'815 Family
16/292,374	U.S. Pat. No. 11,012,529	'815 Family
16/292,382	U.S. Pat. No. 10,447,809	'815 Family
16/365,250	U.S. Pat. No. 10,999,402	'815 Family
16/365,315	U.S. Pat. No. 11,005,967	'815 Family
16/368,002	U.S. Pat. No. 10,582,013	'624 Family
16/368,041	U.S. Pat. No. 10,582,014	'624 Family
16/396,695	U.S. Pat. No. 10,637,968	'624 Family
16/396,696	U.S. Pat. No. 10,637,968	'624 Family
16/524,026	U.S. Pat. No. 11,012,530	'815 Family
16/566,929	Pending	'815 Family
16/567,496	Pending	'815 Family
16/593,996	Pending	'815 Family
16/593,999	Pending	'815 Family
16/600,504	U.S. Pat. No. 11,044,341	'624 Family
16/600,505	Pending	'624 Family
16/600,506	U.S. Pat. No. 11,050,852	'624 Family
16/600,507	U.S. Pat. No. 11,044,342	'624 Family
16/662,800	U.S. Pat. No. 11,044,344	'624 Family
16/662,883	U.S. Pat. No. 10,986,208	'815 Family
16/693,306	U.S. Pat. No. 11,038,989	'624 Family
16/782,073	Pending	'624 Family
16/782,076	U.S. Pat. No. 10,986,216	'624 Family
16/807,661	U.S. Pat. No. 11,044,345	'624 Family
16/807,691	Pending	'624 Family
16/865,362	Pending	'815 Family
16/865,364	Pending	'815 Family
16/865,366	Pending	'815 Family
16/910,724	U.S. Pat. No. 10,785,347	'624 Family
16/910,863	U.S. Pat. No. 10,805,429	'624 Family

16/932,763	Pending	'815 Family
16/932,764	Pending	'815 Family
16/932,766	U.S. Pat. No. 10,979,533	'815 Family
16/932,767	U.S. Pat. No. 11,102,326	'815 Family
17/019,267	Pending	'624 Family
17/019,268	U.S. Pat. No. 10,931,792	'624 Family
17/098,392	U.S. Pat. No. 10,958,768	'624 Family
17/146,625	Issued (patent No. pending)	'815 Family
17/146,649	Pending	'815 Family
17/146,701	U.S. Pat. No. 11,044,346	'624 Family
17/146,728	Pending	'624 Family
17/194,272	Pending	'815 Family
17/194,273	Pending	'815 Family
17/194,336	Pending	'624 Family
17/194,339	Pending	'624 Family
17/241,111	Pending	'815 Family
17/241,113	Pending	'815 Family
17/241,119	Pending	'815 Family
17/331,980	Pending	'624 Family
17/332,001	Pending	'624 Family
17/332,023	Pending	'624 Family
17/332,077	Pending	'624 Family
17/332,116	Pending	'624 Family
17/332,171	Pending	'624 Family
17/332,220	Pending	'624 Family
17/332,260	Pending	'624 Family
17/332,290	Pending	'624 Family
17/395,526	Pending	'624 Family
17/395,926	Pending	'624 Family
17/396,789	Pending	'815 Family
90/014,624	Pending	'624 Family
90/014,652	Pending	'624 Family
90/014,816	Pending	'624 Family
90/014,827	Pending	'624 Family

3. REVIEW OF THE '614 PATENT, ITS ORIGINAL PROSECUTION, AND CLAIMS

3.1. Specification of the '614 Patent

The general architecture of the '614 disclosure is reflected in Fig. 5 of the patent:

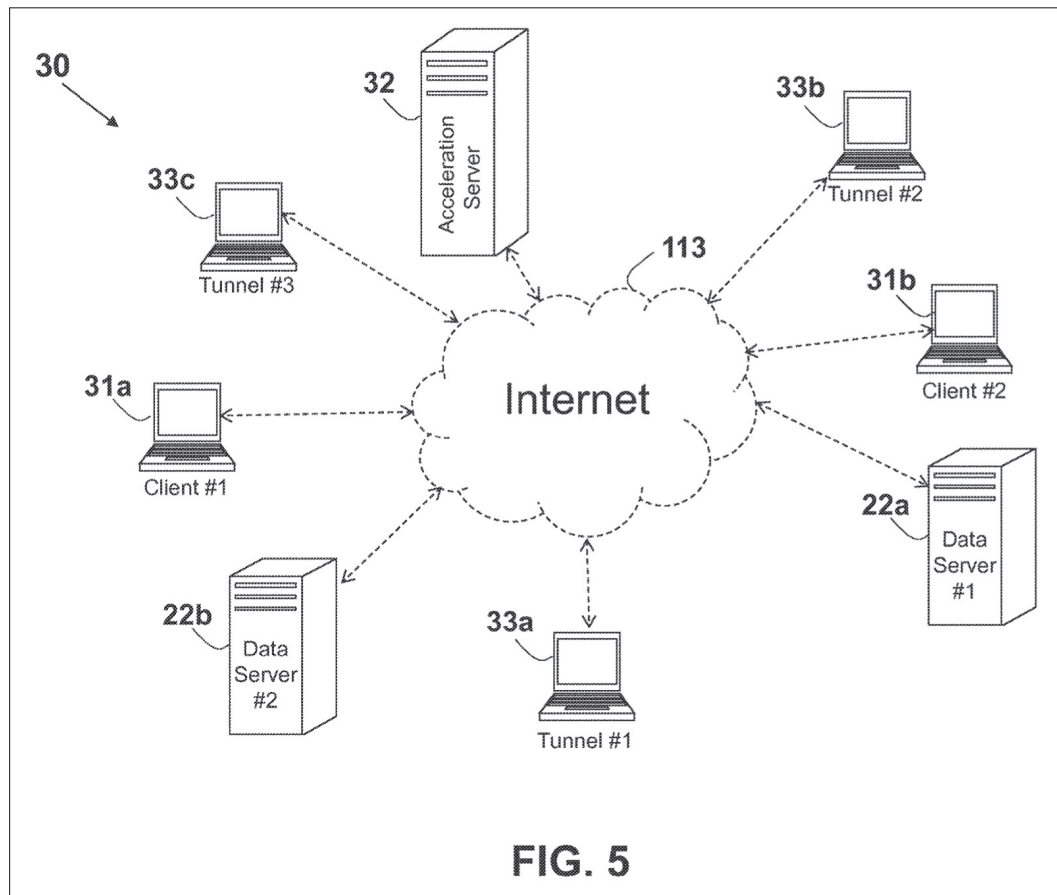


Fig. 5 of the '614 patent

The '614 patent discloses methods for fetching content from a web server, for a client device, using what the patent refers to as “tunnel devices” (33a-c) as intermediate content retrieval agents. A list of tunnel devices available for such retrieval tasks is maintained by an “acceleration server” (32). Ex. 1 at Abstract.

As described in the disclosure, client device 31a seeks to access content that resides on data server 22a (which may be a web server, Ex. 1 at 55:19-24), through an intermediary device, called a “tunnel” device (*e.g.*, 33a).

“Tunnel” devices are described in the '614 patent as follows: “A tunnel device may receive from a client device a request for content from a data

server. Upon receiving such a request, the tunnel device fetches the requested content from the data server and sends the retrieved content to the client device.” Ex. 1 at 66:65-67:2. By receiving a request for content from a client, fetching the content from a data server, and returning the fetched content to the requesting client, these “tunnel devices” of the ’614

patent do exactly what a proxy does—*i.e.*, the “tunnel devices” *are* proxies. Ex. 3 ¶ 41.³

³ The term “tunnel device” is used somewhat confusingly in the ’614 patent, in that, contrary to what a POSITA might at first assume, the term “tunnel” in the context of the ’614 disclosure does *not* necessarily connote protocol “tunneling” as known in the art. See Ex. 3 ¶ 42. The term “tunneling” is commonly understood to refer to a usage in which a first protocol is *encapsulated* within a second, making it appear to the recipient as simply the first protocol, but actually being transported by the second. *Id.* This is done, for example, in a VPN. The specification states (see Ex. 1 at 29:55-30:5) that the tunnel devices *may* have true tunneling (*e.g.*, VPN) connections to the acceleration server (Ex. 1 at 52:52-59), but this feature is only incorporated in a *dependent* claim (claim 5) of the ’614 patent, and not necessary in claim 1. Rather, in the ’614 disclosure, the word “tunnel” refers simply to the option of the requesting device to ask in the first instance for a type of intermediary device that will go *directly* to the origin server for the requested content, as opposed to first searching local caches for that content. See, *e.g.*, Ex. 1 at 29:55-30:5. A “tunnel” in the sense of the ’614 patent thus provides an *option* to *shortcut* (*i.e.*, tunnel through) the local cache retrieval preference of the Shribman ’733 publication—and thereby quite simply to serve as a *proxy* to perform the retrieval directly for the requesting client. This is made most clear in the provisional of the ’614 patent, explaining what it adds to the prior disclosure published as the Shribman ’733 publication:

The “Tunnel” 16 is used by the Client 2 to fetch data from the Data Server 5, when such data is not found in the acceleration network’s elements caches, *or the data is found in the caches but does not make sense for the Client 2 to fetch it for practical reasons, such as because the time to fetch it from the acceleration network’s caches would be longer than to fetch the data directly from the Data Server 5.* In such a case where it is beneficial for the Client 2 to fetch the data directly from the Data Server 5, the Client 2 may use one or more Tunnels 16 to carry out the request to the Data Server 5 on its behalf.

Ex. 5 at 126 (emphasis added). The ’614 patent thus re-prioritizes the retrieval options described in the Shribman ’733 publication (preferring retrieval through a tunnel device rather than an agent device, as in the Shribman ’733 publication). However, as will be addressed herein, the underlying modes of retrieval were all previously disclosed in the Shribman ’733 publication. The ’614 patent also discloses using multiple tunnel devices in parallel (see Ex. 1 at 80:40-43), but this additional feature is not relevant to the ’614 claims.

There are a plurality of tunnel (proxy) devices, 33a-33c (etc.) in the '614 disclosure. Server 32 (referred to as an “acceleration server”) maintains a list of available tunnel devices. Ex. 1 at 82:34-83:1.

The way this arrangement is used in the '614 patent is as follows. Client device 31 signs in with acceleration server 32 (Ex. 1 at 82:34-45) and requests to be allocated a tunnel (proxy retrieval device). Acceleration server 32 responds to client device 31a with the IP address of tunnel device 33a, which will serve as an intermediary for content retrieval (Ex. 1 at 82:34-83:1, 89:19-21). Client device 31a (the allocated “tunnel”) then requests content it desires from data server (origin server) 22a, through tunnel device 33a. Tunnel device 33a acts as an ordinary proxy in this transaction: client 31a sends a content request to tunnel device 33a (Ex. 1 at 83:46-51); tunnel device 33a forwards the content request to data server 22a (Ex. 1 at 83:53-57); data server 22a receives the content request and sends the requested content back to tunnel device 33a (Ex. 1 at 83:57-62); tunnel device 33a returns the requested content to client device 33a (Ex. 1 at 83:62-65). See Ex. 3 ¶ 48.

The exemplary system also has a peer-to-peer aspect, in that the “client” and “tunnel” devices can also readily switch roles. Each tunnel device is loaded with software that can operate as either a client or a server, and thus each tunnel device can also participate in this content retrieval scheme as a client (and vice-versa). Ex. 1 at 95:45-61.

As noted above, in the '614 patent, the acceleration server 32 maintains a list of “available” tunnel devices. The availability aspect ensures that the tunnel devices, to which the acceleration server would assign retrieval tasks, are ready and able to accept the specified retrieval tasks. To reflect its readiness to accept such tasks, each tunnel device can switch

its state based on its online connection status, as well as its availability, as measured internally by metrics such as its memory or CPU utilization. Thus, only tunnel devices determined to be available are assigned retrieval tasks. Ex. 1 at 122:64-123:36.

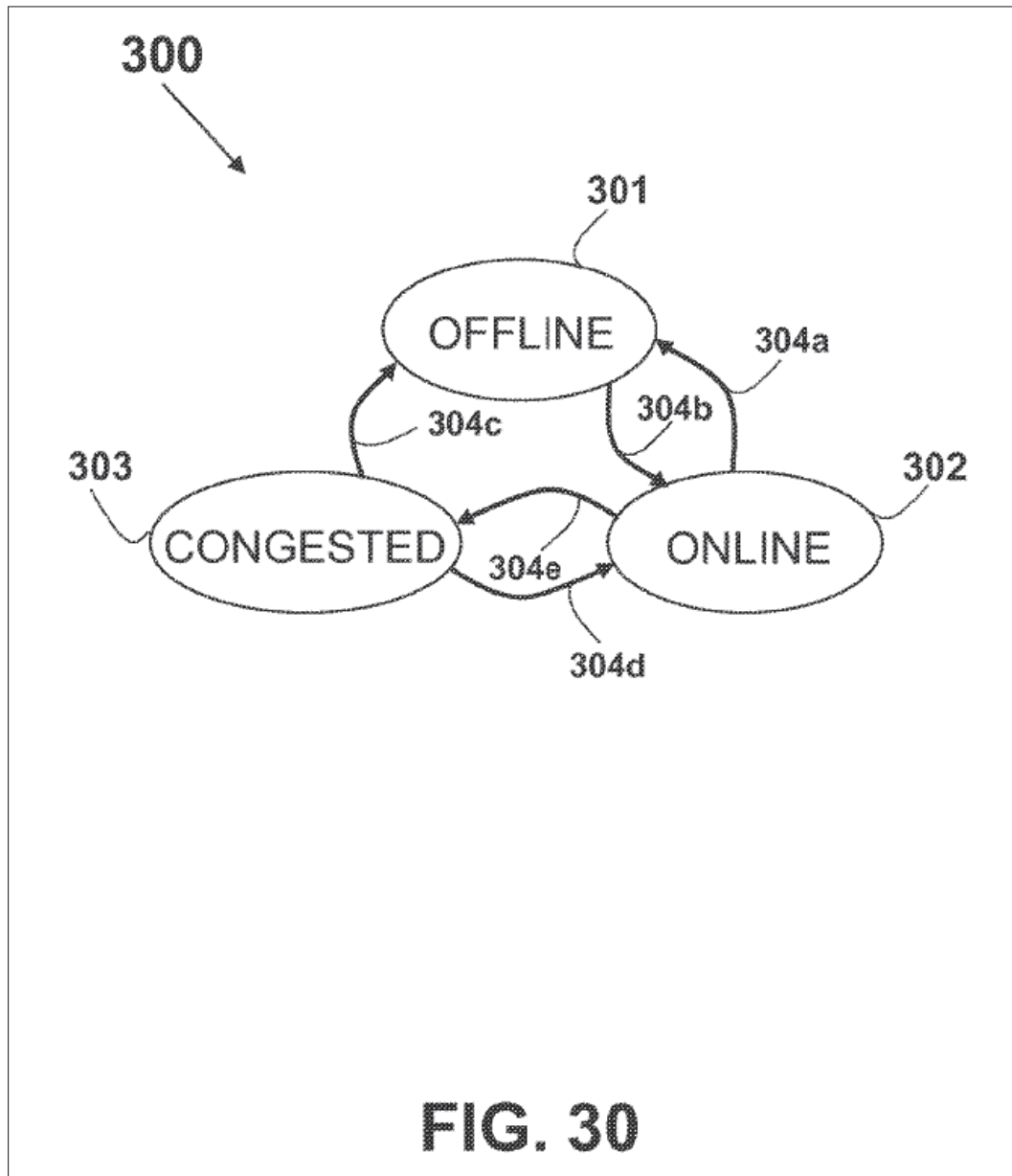


Figure 30 of the '614 patent

As shown in Fig. 30, the tunnel devices depicted in Fig. 5 may be in an OFFLINE, ONLINE, or CONGESTED state (Ex. 1 at 120:34-65, 122:64-123:36), and regularly report/update this status to the acceleration server. “[T]unnel devices that are ‘offline’ and tunnel devices that are congested (such as the tunnel device associated with the entry of the second row 42 b in the table 40) are not used, and are not included i[n] the tunnel devices list sent to the requesting client device.” Ex. 1 at 123:31-35.

Client/Server roles.

The corresponding device in the ’614 specification to the “client device” of the claims is agent 122. The “client device” appears in the claims in a proxy role, *i.e.*, as an intermediate device for retrieving content. In this role as a proxy, agent 122 functions as both a client and a server. Moreover, the device may have an alternate role in the system of the ’614 patent: in the disclosure of the ’614 patent, agent 122 can also at other times assume the role of client 102. Thus, a device functioning as a proxy (and thereby, a server) may be called a “client” (as it is in the ’614 claims), and conversely, a device functioning as a client running a web browser and seeking content may also be referred to as a “server” where it may alternately also function in such a role (such as by also serving as a proxy to retrieve content for other devices).

Under the broad interpretations of “client” and “server” discussed at length in the body of the ’614 patent, those terms (*i.e.*, “client” and “server”) are not mutually exclusive. The same end user computing devices 200 can function as clients or tunnel devices, and may be viewed as either clients and/or servers, depending on the functionality they are carrying out at any given time.

Whether a device has end user functionality is also not determinative with respect to whether it operates as a “client” and/or “server.” The terms “client,” and “server” are used within the disclosure of the ‘614 patent where any device may serve at the same time or at a different time in the role of consuming (client) or providing (server) a service. Thus, in any given deployment, a single device may be capable of performing in both “client” and “server” roles. Consequently, depending on the context, any such device may be referred to as either a client or a server, insofar as it serves in both roles.

Devices such as tunnel devices in the specification *in themselves* incorporate both “client” and “server” functionality. A tunnel device is a server to the client device requesting its services, and also a client to the web server from which it retrieves content. This is reflected in the words of the ‘614 patent itself. See Ex. 1 (‘614 patent), 4:40-61:

The terms ‘server’ or ‘server computer’ relates herein to a device or computer (or a plurality of computers) connected to the Internet and is used for providing facilities or services to other computers or other devices (referred to in this context as ‘clients’) connected to the Internet.

Id. at 4:41-46. The ‘614 disclosure continues, likewise addressing “client” functionality:

Similarly, the term ‘client’ is used herein to include, but not limited to, a program or to a device or a computer (or a series of computers) executing this program, which accesses a server over the Internet for a service or a resource.

Id. at 4:53-57.

The interchangeability of client-server roles is made explicit in the '614 specification itself. See Ex. 1 at 119:50-53 (“[D]evices that are not denoted herein as servers, may equally function as a server in the meaning of client/server architecture.”), 119:18-21 (“[D]evices denoted herein as servers, may equally function as a client in the meaning of client/server architecture.”). This is typified by the fact that the tunnel devices of the '614 patent can function as both clients and servers: they can have separate roles as clients having browsers, and in that capacity request content retrieval from other tunnel devices (each of which also can be a client in its own right).

Moreover, as noted in the preceding paragraphs, even when acting as a proxy retrieval agent, the tunnel device is also a “client” to the web server from which it retrieves content, and a “server” to the other tunnel device for which it retrieves the content. This is necessarily implicit in the '614 patent's above-quoted description of a server as a facility that “provid[es] facilities or services to other computers or other devices,” and a client as a program or device that “accesses a server over the Internet for a service or a resource.” Ex. 1 at 4:46-57. The fact that a device configured as a proxy acts as *both* a client and a server is also explicitly recognized in RFC 2616 (Ex. 12), the specification for the HTTP protocol itself, which is cited repeatedly throughout the '614 specification. RFC 2616 defines a “proxy” as “[a]n intermediary program which acts as *both a server and a client* for the purpose of making requests on behalf of other clients.” Ex. 12, RFC 2616 at 10 (emphasis added).

Thus, the terms “client” and “server” as used in the '614 patent are intentionally broad. Whether a device qualifies as a “client” and/or a “server” for purposes of the claims of the '614 patent depends only on whether it

is capable of functioning as such, either in the same capacity in which it appears in the claim, or in a alternate capacity, which could be at an alternate time.

Furthermore, in a client-server architecture, tasks may be divided between the client and the server. The '614 patent discusses as prior art the use of inter-process communication (IPC), such as remote procedure calls (RPC), which can be used in this manner, to shift specified processing from client to server, or vice-versa. *See* Ex. 1 at 36:14-19. A difference between two references concerning on which side of a client-server relationship a given piece of processing is performed may often be a mere design choice. That is because the processing in question can readily be shifted from one side of the client-server relationship to the other, using well-known techniques such as RPC. *See* Ex. 3 ¶ 60.

3.2. Overview of the '614 Patent Claims

The '614 patent has only one independent claim, which is claim 1 (the numeric references to the claim steps, in square brackets, have been inserted by the Requester, for purposes of reference):

[1.P] A method for use with a resource associated with a criterion in a client device that communicates with a first server over the Internet, the client device is identified in the Internet using a first identifier and is associated with first and second state according to a utilization of the resource, the method comprising:

[1.1] initiating, by the client device, communication with the first server over the Internet in response to connecting to the Internet, the communication comprises sending, by the client device, the first identifier to the first server over the Internet;

[1.2] when connected to the Internet, periodically or continuously determining whether the resource utilization satisfies the criterion;

[1.3] responsive to the determining that the utilization of the resource satisfies the criterion, shifting to the first state or staying in the first state;

[1.4] responsive to the determining that the utilization of the resource does not satisfy the criterion, shifting to the second state or staying in the second state;

[1.5] responsive to being in the first state, receiving, by the client device, a request from the first server; and

[1.6] performing a task, by the client device, in response to the receiving of the request from the first server,

[1.7] wherein the method is further configured for fetching over the Internet a first content identified by a first content identifier from a web server that is distinct from the first server, and the task comprising:

[1.8] receiving, by the client device, the first content identifier from the first server;

[1.9] sending, by the client device, the first content identifier to the web server;

[1.10] receiving, by the client device, the first content from the web server in response to the sending of the first content identifier; and

[1.11] sending, by the client device, the received first content to the first server.

Claim 1 recites the following objects, conditions, and actions:

a client device	Where “client” is very broadly defined based on the role performed by the device
a resource and a criterion	A resource associated with the client (proxy) device, and a criterion reflecting utilization of the resource
first and second state	Possible states of the client (proxy) with respect to utilization of the resource (<i>e.g.</i> , Online/Available/Accepting, Congested/Unavailable/Unaccepting)
a first server	A server (very broadly defined, could be any devices that acts as a server), that is accessible over the Internet
first identifier	Identifies the client (proxy) device on the Internet
a request	A request from the first server to the client (proxy) device, which the client receives if it is in an accepting state
a task	A content retrieval task performed by the client (proxy), responsive to receiving the request
a web server	Any web server distinct from the first server, which is accessible over the Internet
a first content identified by a first content identifier	Content to be retrieved from the web server by the client (proxy) device and sent by it to the first server

The devices recited in the claims are ordinary devices that exchange standard Internet requests or content in a routine way. Claim 1 recites the “client device” as an intermediary (proxy), where the “client device”—after it is confirmed as available based on its utilization of resources—acts as an intermediary to retrieve from a web server content requested by a “first server,” and send the content to the first server.

The dependent Challenged Claims recite well-known modes of implementation and configuration, such as that “TCP/IP” is used, that the client device uses a standard operating system (either desktop or mobile), itemizing the types of devices that can serve as “client devices,” and so forth. These dependent claim features will also be addressed herein as necessary.

Since the grounds for *ex parte* reexamination are limited to unpatentability over patents and printed publications, Requester takes no position herein with respect to other potential issues of validity, such as the adequacy of the written description or the definiteness or indefiniteness of the claims. (Such issues may of course also exist, but are beyond the scope of this submission.)

3.3. Correspondence of Claims to the '614 Specification—Mapping the '614 Patent to Itself

While not necessarily limiting, Requester suggests that it is helpful, in order to better understand the claims, and claim 1 in particular, and how corresponding elements may be reflected in the prior art, to identify how claim 1 corresponds to the written description of the '614 patent itself (to the extent support exists within the written description). This is as follows:

1. A method for use with a resource associated with a criterion in a client device that communicates with a first server over the Internet, the client device is identified in the Internet using a first identifier and is associated with first and second state according to a utilization of the resource, the method comprising:

Client device: E.g., tunnel #1 (33a).

Resource: E.g., a capability such as “storage capacity, I/O activity, CPU utilization, or available communication bandwidth” (Ex., 75:5-12; 121:13-32).

Criterion: use of the resource “over a certain threshold” (Ex. 1, 75:8-9; 121:13-32).

First server: E.g., Client #1 (31a). (Note that the first server *cannot* be acceleration server 32 for at least the reason that there is no disclosure anywhere in the written description that the acceleration server ever receives actual web content as recited in the last step of this claim—which rules out acceleration server 32 as corresponding to the “first server” in this claim.)

First identifier: E.g., Client #1 IP address. 84:29-32 (“The [sign-in] message comprises the device functionality as ‘client’, and the device 31a identification on the Internet 113, such as its IP address (for example 36.83.92.12).”).

First and second state according to utilization of the resource: E.g., the “Online,” “Offline,” and “Congested” states as shown in Fig. 30.

initiating, by the client device, communication with the first server over the Internet in response to connecting to the Internet, the communication comprises sending, by the client device, the first identifier to the first server over the Internet;

Client device 31 signs in with acceleration server 32 (Ex. 1 at 82:34-45). Note that in this communication, the client device sends its own IP address to the acceleration server. It is later relayed to the device regarded as the “first server.” These are the only disclosures addressing this limitation. The disclosure in support of this limitation is thus indirect—constituting (1) communication of the client IP address by the client to the acceleration

server, followed by (2) a subsequent communication of the client IP address by the acceleration server to the first server. *See* Ex. 1, 108:67-109-19. There is no written description disclosure of any *direct* sending by the device regarded as the first client device in this claim of its own IP address to the device regarded as the first server.

when connected to the Internet, periodically or continuously determining whether the resource utilization satisfies the criterion;

E.g., 120:47-49 (“The device monitors its resources and performance, and upon detecting a resource utilization that is above a set threshold, declares itself as congested.”)

responsive to the determining that the utilization of the resource satisfies the criterion, shifting to the first state or staying in the first state;

See discussion of state diagram 300 (Fig. 30), Ex. 1, 120:34-121:12.

responsive to the determining that the utilization of the resource does not satisfy the criterion, shifting to the second state or staying in the second state;

Id.

responsive to being in the first state, receiving, by the client device, a request from the first server; and

Ex. 1, 122:42-46; 124:3-30.

performing a task, by the client device, in response to the receiving of the request from the first server,

E.g., Ex. 1, 126:18-22 (“execute the tunnels-using client device flowchart”).

wherein the method is further configured for fetching over the Internet a first content identified by a first content identifier from a web server that is distinct from the first server, and the task comprising:

receiving, by the client device, the first content identifier from the first server;

E.g., Ex. 1, 'Content Request' message 56g; 85:42-45 ("The request is received at the tunnel device #1 33a at a 'Request Received' state 54c, corresponding to a 'Receive Content Request' 73b in the flowchart 70)").

sending, by the client device, the first content identifier to the web server;

E.g., *id.* 85:45-48.

receiving, by the client device, the first content from the web server in response to the sending of the first content identifier; and

E.g., *id.* 85:49-54.

sending, by the client device, the received first content to the first server.

E.g., *id.* 85:54-57.

3.4. Priority Date

The '614 patent claims priority to provisional application 61/870,815 filed August 28, 2013. The prior art references asserted herein pre-date that date; Requester does not contest (for purposes of this Request only) the claimed priority date of August 28, 2013 ("Priority Date"). As noted above, the claimed priority is after March 16, 2013, thus making the '614 patent subject to the first-inventor-to-file provisions of the AIA.

3.5. Prosecution History of the '614 Patent, and Reasons for Allowance

The application for the '614 patent was filed under Track 1 on December 10, 2018, as a continuation of application No. 16/140,785, filed on September 25, 2018, ultimately claiming priority of Provisional application No. 61/870,815, filed on August 28, 2013.

The application was filed with one independent and 29 dependent claims, for a total of 30 original claims.

The file wrapper is reproduced in Ex. 2 and referred to by page number as represented in that Exhibit. Independent claim 1 (*see* Ex. 2 at 669) recited substantially the steps of monitoring a client device for resource utilization, and shifting states accordingly, to determine whether to have the client perform a task, but leaving the task unspecified. As originally filed, claim 1 did *not* include any recitation regarding the particular task to be performed by the client device being monitored for its state of availability.

The first action (Ex. 2 at 541) was a nonfinal rejection of claims 1-10 and 13-28 under 35 U.S.C. § 103, over Sigurdsson (Ex. 7) in view of Chauhan (Ex. 8). The Examiner found that Sigurdsson disclosed all limitations of original claim 1 other than the client initiating communication with the server over the Internet in response to powering up, for which it relied on Chauhan. The Examiner rejected claims 2-10 and 13-28 on similar bases. The Examiner rejected claims 11-12 (concerning mobile device implementations) further in view of Bhatia (Ex. 17), and rejected claims 29 and 30 (combinations similar to issued claim 1) further in view of Deng.

The applicant traversed (Ex. 2 at 508). The next action was final (Ex. 2 at 471). In response, the applicant filed an RCE and amended (Ex. 2 at

462), primarily to recite that the task is performed in response to receiving a request from the [first] server, but still not specifying the task. This was followed by a nonfinal rejection, which added Jackowski (Ex. 9) as a further reference, specifically as to step [1.5] (responsive to being the the first state, receiving, by the client device, a request from the server and performing a task). Ex. 2 at 373-374.

The applicant made another minor amendment and otherwise traversed (Ex. 2 at 334), leading to another final rejection (Ex. 2 at 283), which added further grounds of rejection based on Sigurdsson and indicated allowable subject matter as to claim 28 (if in independent form), which added the feature of the client device also reporting its geographic location.

The applicant amended to incorporate the limitations of claim 29 into claim 1 (and cancel claim 29). See Ex. 2 at 197. The Examiner noted some informalities in the amendment (Ex. 2 at 132 (advisory action)), the applicant resubmitted the amendment (Ex. 2 at 117), which was followed by an Examiner's amendment and an allowance. Ex. 2 at 17-23. The reasons for allowance also noted what the Examiner considered the closest prior art (which included Dorso).

Ex. 18 is a redline comparison of claim 1 as originally filed, against the claim as issued, after the applicant amended claim 1 to incorporate the limitations of claim 29. Requester submits that it is clear from the redline, which reflects the net change in claim 1 over the course of prosecution, that it was the *combination* of (i) the original limitations, which concerned monitoring client devices to be used to perform a task, with (ii) further limitations spelling out that the task to be performed was to provide retrieval

of content from a web server over the Internet, that led to the allowance (confirming the Examiner's statement to the same effect).

Also in the prosecution history is a record of prior art submissions. In an IDS submitted upon filing, the applicant listed its own U.S. 8,560,604 patent (Ex. 2 at 818).

The '604 patent (also discussed in the '614 specification) issued on October 15, 2013, *after* the claimed priority date of August 28, 2013.

Because the issue date of the '604 patent was after the effective filing date of the '614 patent, the disclosed '604 patent is not prior art to the '614 patent under 35 U.S.C. § 102(a)(1).

35 U.S.C. § 102(a)(2) does not apply to the '604 patent as potential prior art to the '614 patent because the inventorship was identical to that of the '614 patent.

Thus, the original IDS disclosure of the '604 patent was of an item that did not qualify as prior art.

The original IDS submitted in the case (Ex. 2 at 817) did *not* disclose the Shribman '733 publication, despite the fact that it was by the *same inventors* as in the pending '614 application in which the IDS was submitted, and despite the fact that the Shribman '733 publication clearly constituted "printed publication" prior art under 35 U.S.C. § 102(a)(1) and concerned highly similar subject matter.

To perceive the existence of the Shribman '733 publication as prior art, based on the applicant's originally filed IDS, the Examiner would have had to look behind the citation of the '604 patent and realize that its earlier publication was the Shribman '733 publication, published April 14, 2011 and thus that the publication (*not itself listed in the IDS*) constituted prior art as a "printed publication" under 35 U.S.C. § 102(a)(1).

To recap, the Shribman '733 publication itself was not listed in the IDS filed with the application on December 10, 2018. Rather, the Shribman '733 publication was *eventually* identified in a *later filed* IDS (Ex. 2 at 447). However, that **subsequent** IDS submission was not until March 24, 2019, when the later IDS was filed along with the RCE filed after the first two actions on the application for the '614 patent.

Though the Shribman '733 publication was eventually placed before the Examiner during original prosecution, it was not placed before the Examiner as clearly as it might have been, given its late filing without explanation and the fast track nature of the Track 1 proceeding. Though the IDS entry for the Shribman '733 publication was initialed on the IDS form (Ex. 2 at 388), the Shribman '733 publication was not discussed by either the Examiner or the applicant on the record, nor was it applied in any action, either by itself or in any combination. It was only one of 27 references submitted, without any comment or indication of relevance, in the particular IDS. It can be seen, therefore, how the Shribman '733 publication, though highly relevant, may have avoided the Examiner's in-depth attention in the original examination.

Likewise, neither the Mithyantha or MorphMix references further cited herein was raised during original prosecution.

3.6. Claim Construction

3.6.1. Claim Construction Standard

The '614 patent is unexpired and accordingly its claims should be given the broadest reasonable interpretation ("BRI") in light of the specification. *In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984); MPEP 2258(I)(G).

3.6.2. Prior District Court *Markman* Rulings

Exs. 15 and 30 are an E.D. Tex. decision and a supplemental decision, respectively, construing terms of the '614 patent. See MPEP 2111 (“Patented claims are not given the broadest reasonable interpretation during court proceedings involving infringement and validity In contrast, an examiner must construe claim terms in the broadest reasonable manner during prosecution as is reasonably allowed in an effort to establish a clear record of what applicant intends to claim. Thus, the Office does not interpret claims when examining patent applications in the same manner as the courts.”) (citations omitted). Most of the court’s constructions were plain and ordinary meaning. It confirmed the parties’ agreed construction of the preamble of claim 1 as limiting.

Only two specific constructions were provided for the '614 patent, and these were of the terms “client device” and “first server”:

Term	Court’s Construction
“client device”	“device operating in the role of a client by requesting services, functionalities, or resources from the server” (Ex. 15 at 15)
“first server”	“server that is not the client device” (Ex. 15 at 16)

In response to an assertion of the indefiniteness of the term “sequentially executed” in claim 7, the court found the claim not to be indefinite but that it “require[d] the ten steps of Claim 1 [from which claim 7 depends] to be performed in the recited order.” Ex. 15 at 23.

As to “client device,” the court cited Patent Owner’s extrinsic evidence, the W3C Glossary of Terms for Device Independence. See Ex. 31 at 4; Ex. 15 at 12. In IPRs concerning Patent Owner’s related patents, the Board

construed “client device” in almost these exact terms, as “a device that is operating in the role of a client by requesting services, functionalities, or resources from other devices.” Ex. 36, IPR2021-00458, Paper 11 at 19 (Institution Decision, concerning Patent Owner’s Patent No. 9,241,044). *See also* Ex. 37, IPR2021-00465, Paper 11 at 14-15 (same, concerning Patent Owner’s Patent No. 9,742,866).

In its supplemental ruling (Ex. 30), the court reaffirmed that “a component can be *configured* to operate in different roles.” Ex. 30 at 10 (emphasis in original). The supplemental ruling also confirmed as correct the interpretation that its prior ruling meant that the “first server” of the ’614 patent claims could be construed as “a device that is operating in the role of a server by offering information resources, services, and/or applications and that it is not the client device” (Ex. 30 at 8 & 11)—an interpretation consistent with Requester’s position herein.

At a subsequent pretrial conference, in a ruling that could prove significant with respect to arguments the Patent Owner may seek to raise in this reexamination, the court further instructed that, in view of its rulings with respect to the role-based interpretation of what is a client and what is a server, that the Patent Owner’s expert would not even be *permitted* to testify “that a client device is specifically not a server.” Ex. 32 at 64.

In IPR2021-00458, concerning Patent Owner’s patent No. 9,241,044 (similar in substance, though claiming later priority), the Board construed “server” in a similar manner, as a “program accepting and servicing requests from clients; a server may be an origin server or a proxy server.” Ex. 36, IPR2021-00458, Paper 11 at 21.

These rulings leave no latitude for the Patent Owner to contend that acting as a client rules out the same device from also acting a server,

or vice-versa. Any such arguments, should they be made by the Patent Owner during this reexamination, would have no basis in the literal claim language, would be contrary to court and PTAB rulings on the '614 patent, and contrary to clear disclosures in the specification, and thus should be given no weight.

3.6.3. Requester's Claim Construction Positions Herein

Prior court claim construction ruling

Requester agrees with the court's interpretation of the claims as set forth in Ex. 15, Ex. 30, and Ex. 32, and believes these interpretations are consistent with a BRI construction. In particular, Requester submits that the court's constructions of "client device" and "first server" are consistent with the BRI and appropriate for purposes of reexamination in the USPTO.

"client device"

The court construed "client device" as a "***device operating in the role of a client by requesting services, functionalities, or resources from the server***"—specifically rejecting the Patent Owner's proposal that the term "client device" must be understood as limited to "a device using a client dedicated operating system and operating in the role of client by requesting services, functionalities, or resources from the server". Ex. 15 at 14-15 and 23.

Thus, a device that may have some other role in the system may nevertheless be regarded as a client device to the extent that it also operates in the role of a client, in the context of the claim, in "requesting services, functionalities, or resources from the server." This is indeed what is disclosed in the '614 patent, where a "tunnel device" (*e.g.*, 33a) acting as a content retrieval proxy, thereby requests a "resource" (*i.e.*, content identi-

fied by a Uniform Resource Identifier (URL)) from the server, in this case, the “data server” 22a (the “web server” in claim 1) . Ex. 1 at 85:34-86:3. The “Tunnel device” is thus a client relative to the server from which it requests the content resource. In terms of claim 1, Tunnel 33a in Fig. 5 of the ’614 patent operates in the role of a client device, within the meaning of the court’s construction, even though it may also operate in the role of a server.

“first server”

The court interpreted “first server” to mean “server that is not the client device.” Ex. 15 at 16, 24.

In its supplemental ruling (Ex. 30), the court reaffirmed that “a component can be *configured* to operate in different roles” (Ex. 30 at 10 (emphasis in original)), and confirmed as correct a “role-based” interpretation of what is a “server,” *i.e.*, the interpretation that the “first server” for purposes of the ’614 claims may be understood as “a device that is operating in the role of a server by offering information resources, services, and/or applications and that it is not the client device” (Ex. 30 at 8, 11).

At a subsequent pretrial conference, the court further instructed that Patent Owner’s expert could not testify “that a client device is specifically not a server.” Ex. 32 at 64.

In IPR2021-00458, concerning Patent Owner’s patent No. 9,241,044 (similar in substance, though claiming later priority), the Board construed “server” in a similar manner, as a “program accepting and servicing requests from clients; a server may be an origin server or a proxy server.” Ex. 36, IPR2021-00458, Paper 11 at 21.

In the context of the ’614 disclosure, “the” client device for purposes of the operations of claim 1 would be the Tunnel device. The content re-

quest comes to the Tunnel device 33a from client 31a. Client 31a is not “the” client device in this operation (Tunnel 33a is). But despite also being labelled as a client, client 31a is nevertheless also a server. It is a server because in addition client 31a also serves in the disclosure as a Tunnel device in its own right, and thus as a “server” to other “clients.” This understanding is consistent with the disclosure, and indeed the only interpretation under which claim 1 would read on any disclosed embodiment in the ’614 patent.

It is therefore clear from the court’s several rulings that no special meaning should be attached to the term “first server” that requires anything more than what the court specified. Thus, ***a “first server” may be regarded as a device that has at least a role in which it operates as a server in the system in question, provided only that it is not the same device as the device serving as the client device in carrying out the claim steps.***

“resource”

This term was not construed by the court. Requester takes the position that, consistent with the BRI, the term “resource” should be understood to include not just an individual facility of a device (CPU, memory, bandwidth, etc.), but the collected available input and output capacities at the client device.

The Examiner’s view of Sigurdsson during the original examination of the ’614 patent confirms the appropriateness of this broad interpretation of the term “resource.” Rejecting the applicant’s argument that Sigurdsson “fail[ed] to teach a client device periodically or continuously determining a state based on the resource,” the Examiner stated that Sigurdsson “discloses monitoring or polling, by the client, to determine the client’s

status [and] to determine if the client is offline or online [where] a client determin[ed] that a peer client had a bandwidth (resource utilization) that exceeds a predetermine[d] value.” Ex. 2 at 285-86 (applying the BRI and citing ¶¶ [0008], [0061], and Fig. 8, element 804 of Sigurdsson). The Examiner further explained that Sigurdsson taught “for use with a set threshold value, and wherein the criterion is satisfied when the resource utilization is above or below the threshold,” using the BRI where Sigurdsson “disclose[d] transmitting data between clients only in the event that a peer client doesn’t have bandwidth that exceeds a predetermined threshold.” *Id.* at 287 (citing ¶¶ [0008], [0012]).

However, the Examiner did not limit its interpretation of Sigurdsson’s disclosure of the “resource” term to bandwidth utilization. Specifically, the Examiner stated:

Note that the term resource has been mapped to bandwidth utilization and **throughput of a client device**. One of ordinary skill in the art (using the broadest reasonable interpretation of a resource comprises, or consists of, **input or output capability**), [would consider] the collected available resource capacities at each client device (par [0051], lines 10-11 of Sigurdsson et al) because analyzing client devices for available resource capacities would require for [sic] analysis of internal components within each client device, which discloses various input/output components (as disclosed in fig. 1, 4, and 9 of Sigurdsson et al.

Id. at 288 (emphasis added).

Therefore, consistent with the ’614 prosecution history and the BRI, ***the term “resource” should be understood to include not just individual resources, but the collected available input and output capacities at the client device.***

“state”; “shifting” state

The court did not construe the terms “state” or “shifting” state.

A “state” of a system or device is ordinarily understood as the remembered situation of the system or device based on previous inputs. See Ex. 3 ¶ 77.⁴ Under the broadest reasonable interpretation, such a state may be reflected in a text or database entry that is set in accordance with input and which persists for some time after being so set.

Likewise, **a “shift” from a first state to a second state may be understood as requiring nothing more than that the first and second situations (states) are well-defined and distinguishable, and that one such situation follows in time from the other.** While this may be satisfied by formal “state” definitions, as in an explicitly defined “finite state machine,”⁵ under BRI it should be sufficient that the input results in, for example, a definite, persistent record stored (e.g., written) in the

⁴ See also, e.g., Ex. 13 at 158 (“Squid keeps a variety of statistics and state information about each of its neighbors. One of the most important is whether Squid thinks the neighbor is *alive* (up) or *dead* (down). The neighbor’s alive/dead state affects many aspects [of] Squid’s selection procedures. The algorithm for determining the alive/dead state is a little bit complicated”) (emphasis in original), 339 (“Squid marks each of its peers as either dead (down) or alive (up). Squid uses ICP/HTCP replies (and other techniques) to determine a peer’s state. If Squid doesn’t receive any replies for the time specified by *dead_peer_timeout*, the peer is declared dead. . . .As soon as Squid receives an ICP/HTCP reply from a dead peer, its state is changed to alive.”).

⁵ See, e.g., Ex. 35 at 4:

Finite-state machines constitute a very general class of functions. Any transduction which can be represented by a finite number of input symbols being mapped into a finite number of output symbols in a finite number of mutually exclusive ways is a finite-state machine. That is to say, the response of a finite-state machine to any particular input symbol depends not only upon that symbol but upon the internal state of that machine at the time it receives the input symbol.

device, which is distinguishable from the corresponding record resulting from other inputs. For example, some record that survives the event of the input itself, of some condition of the device being on, off, live, dead, available, accepting or not accepting input, online, offline, congested, etc.

This interpretation is consistent with the Examiner's interpretation during the original examination of the '614 patent. For example, the Examiner interpreted Sigurdsson to "collect[] available resource capacities on the one hand and to collect client device status, e.g., 'online or offline status of each client," on the other. Ex. 2 at 288-89.

Order of method steps

Requester notes that all claims of the '614 patent are method claims, and that there is a presumption that unless the claim language clearly requires otherwise (see dependent claim 7, which recites "sequential" order), the steps of a method claim need not necessarily be performed in the order in which the steps are stated in the claim. See *Interactive Gift Exp., Inc. v. Compuserve, Inc.*, 256 F.3d 1323, 1342 (Fed. Cir. 2001) ("Unless the steps of a method actually recite an order, the steps are not ordinarily construed to require one.") (citations omitted); cf. Ex. 30 at 23.

4. OVERVIEW OF THE SUBMITTED PRIOR ART

4.1. Shribman '733 publication (Ex. 6)

United States Patent Publication No. 2011/0087733 to Shribman *et al.* (the "Shribman '733 publication") (Ex. 6) was published by the '614 inventors on April 14, 2011, more than one year before the earliest claimed priority date of the '614 patent, and thus qualifies as printed publication prior art under 35 U.S.C. § 102(a)(1). Although the Shribman '733 pub-

lication represents similar prior work by the same inventive entity, and was discussed in the August 28, 2013 provisional patent application (Ex. 5) that led to the '614 patent, the '614 patent does not purport to claim priority to any of the patent applications underlying Shribman '733 publication. The '614 patent's earliest claimed priority date is August 28, 2013, and the Shribman '733 publication, having been published on April 14, 2011, is printed publication prior art to the '614 patent.⁶

The Shribman '733 publication is similar to the disclosure of the '614 patent, architecturally. It discloses deploying a geographically diverse array of peer devices that can interchangeably function as clients, peers, or agents (caching proxies). As in the '614 patent, each of these devices also get to participate in the arrangement in the role of clients, and using the provided arrangement of devices, the Shribman '733 publication likewise claims to provide more efficient retrieval of content from origin servers over the Internet. While the Shribman '733 publication uses what it calls "agent" devices for content retrieval, as opposed to what the '614 specification calls "tunnel" devices, its agent devices, as will be discussed, also act in a client capacity and therefore qualify as "client devices" for purposes of the present claims (which in any case do not use the term "tunnel").⁷

⁶ Because the Shribman '733 publication, though by the same inventors, predates the earliest claimed priority date of the '614 patent by more than one year, none of the exceptions to 35 U.S.C. § 102(a)(1) as set forth in 35 U.S.C. § 102(b) ("Disclosures made 1 year or less before the effective filing date of the claimed invention") are applicable.

⁷ As discussed in the provisional application underlying the '614 patent, the '614 patent adds "tunnel" devices to the client, peer, and agent devices of the Shribman '733 publication. Ex. 5 at 126. The "tunnel" devices provided a direct client-to-web server path for proxied retrieval. *Id.* The Shribman '733 publication provided that the "agent" devices could perform in that role where the agent determined that the requested content had not previously been cached by any of the peers. See discussion in Section 7 below.

The Shribman '733 publication was first cited in an IDS submitted with an RCE well after the initial filing. The Shribman '733 publication was not applied in any office action, nor does the record reflect that the Shribman '733 publication was discussed in any context by either the Examiner or the applicant. While it was initialed on the IDS, there is no indication in the record that the Examiner considered the particular combination of the Shribman '733 publication with Sigurdsson, Chauhan, or any of the other art cited in the rejections that the Examiner made.

4.2. Liu (Ex. 29)

Liu, U.S. Patent Pub. No. 2010/0082513 A1 ("Liu"), was published on April 1, 2010 and is prior art. Liu concerns the detection and prevention of denial of service attacks in dynamic distributed systems, including peer-to-peer (P2P) environments, mobile networks, and grid computing environments. See Ex. 29 ¶ [0027]. Liu further describes an information layer agent that determines if events indicate attacks, for example, by consulting a knowledge base comprising information associated with known attack patterns, including state-action mappings. See *id.* at Abstract. Liu was not before the Patent Office during prosecution of the '614 patent. See Ex. 2.

4.3. Sigurdsson (Ex. 7)

Sigurdsson *et al.*, U.S. Patent Pub. No. 2007/0174246 A1 ("Sigurdsson"), was published on July 26, 2007 and is prior art. Sigurdsson was cited and applied in the original examination.

4.4. Chauhan (Ex. 8)

Chauhan *et al.*, U.S. Patent Pub. No. US2010/0262650 A1 (“Chauhan”), was published on October 14, 2010 and is prior art. Chauhan was cited and applied in the original examination.

4.5. Bhatia (Ex. 17)

Bhatia *et al.*, U.S. Patent Pub. No. US2013/0171964 A1 (“Bhatia”), was published July 4, 2013 and is prior art. Bhatia was cited and applied in original examination.

4.6. Ebata (Ex. 23)

Ebata *et al.*, U.S. Patent No. 6,513,061 (“Ebata”) (Ex. 23), issued on January 28, 2003 and thus is prior art under 35 U.S.C. § 102(a)(1). Ebata concerns selection of proxies based on, inter alia, their geographic location. See Ebata, Abstract (“proxy server selecting server notifies the client of the IP address of the most approximate server to the client in place of the IP address of the server, based on the physical/logical location information”). Ebata was not before the Patent Office during prosecution of the ’614 patent. See Ex. 2.

4.7. Mithyantha (Ex. 10)

United States Patent 8,972,602, to Mithyantha (“Mithyantha”), Ex. 10 is similar to the ’614 patent, in that Mithyantha also concerns distributing network traffic over a plurality of devices which may be interconnected, where some of the devices may be regarded as clients, and others of which may be regarded as servers, depending on the role that the respective devices are assigned to play in the traffic distribution scheme. Mithyantha

issued on March 3, 2015, and names inventors other than those named in the '614 patent. Mithyantha's application 13/524,799 was filed June 15, 2012, prior to the March 28, 2013 effective filing date of the '614 patent. Accordingly, Mithyantha is prior art under 35 U.S.C. § 102(a)(2) (AIA).

Mithyantha was not before the Patent Office during prosecution of the '614 patent. *See* Ex. 2.

Requester does note that there is some commonality among Mithyantha, submitted herewith, and each of Chauhan and Jackowski, which were considered and applied during original prosecution as also discussed herein. Mithyantha is commonly assigned with, and shares some disclosure with Chauhan (Ex. 8) and Jackowski (Ex. 9). Mithyantha was a later application from the same company (Citrix Systems Inc.), which did not claim priority to Chauhan or Jackowski or any application with common priority to Chauhan or Jackowski. Doc-to-doc comparisons of the specifications of Mithyantha with that of Chauhan and Jackowski, respectively, are submitted as Exs. 8 and 9 herewith. These comparisons show that three references share an essentially common introductory disclosure, including some of the same figures *at the beginning* of the respective documents. However, after this common base, the three documents diverge: In the case of Chauhan, at least ¶¶ [0232]-[0300] of Chauhan do *not* appear in Mithyantha, and at least the matter from 51:31 to 60:55 of Mithyantha does *not* appear in Chauhan. In the case of Jackowski, at least ¶¶ [0195]-[0233] of Jackowski do *not* appear in Mithyantha, and at least the matter from 33:45 to 60:45 of Mithyantha does *not* appear in Jackowski. As will be seen, though this introductory overlap exists, this Request relies in particular on disclosures in cols. 56-57 of Mithyantha, which are separate and apart from the content of either Chauhan or Jack-

owski. Conversely, this request also relies on disclosures from paragraphs of Chauhan numbered higher than [0231], which likewise have no counterpart in Mithyantha. Thus, Chauhan and Jackowski (each cited in the original examination) and Mithyantha (newly cited here) are to a large extent separate, non-cumulative references as cited and relied upon in this Request.

4.8. MorphMix (Ex. 11)

MorphMix—A Peer-to-Peer-based System for Anonymous Internet Access (“MorphMix” (Ex. 11))—is a doctoral thesis authored by Marc Rennhard, of the Swiss Federal Institute of Technology, Computer Engineering and Networks Laboratory; Zurich, Switzerland. MorphMix states it was published in 2004. Dr. Rennhard, his supervisor Dr. Plattner, and the Swiss National Library, each confirmed in declarations that MorphMix was published in 2004. Ex. 21; Ex. 3 ¶ 92. MorphMix is accordingly prior art. 35 U.S.C. § 102(a)(1). MorphMix was not before the Patent Office during prosecution of the '614 patent. See Ex. 2.

4.9. RFCs 2616, 791, and 793 (Exs. 12, 22, and 28)

Request for Comments (“RFC”) (and like standards documents) posted on the Internet are published in the ordinary course by established standards organizations, and are intended to be widely viewed by the interested Internet engineering audience as of their dates of publication as stated on the cover of each.

RFC 2616 (Ex. 12), by R. Fielding *et al.*, was a definitive specification for the HTTP/1.1 protocol. RFC 2616 was published by the HTTP Working Group of the Internet Engineering Task Force (IETF) in June 1999. RFC

2616 is discussed in the '614 patent specification and was submitted during prosecution of the '614 patent, but the prosecution history does not reflect that RFC 2616 was applied by the Examiner in the original examination of the claims. Ex. 1, 4:67-5:1, 5:62-64; Ex. 11, p. 566 (IDS listing RFC 2616 as prior art).

RFC 791 (Ex. 22), by J. Postel (Ed.), published in September 1981, defines the Internet Protocol (IP), a foundational specification for the Internet.

RFC 793 (Ex. 28), by J. Postel (Ed.), also published in September 1981, defines the Transmission Control Protocol (TCP), a connection-oriented end-to-end protocol using IP packets as specified in RFC 791, which is also foundational to the Internet.

See Ex. 3 ¶¶ 93-96.

4.10. Standard Practices for Application Startup Configuration

As of the time of the earliest claimed priority date of the '614 patent, a POSITA would also have been well familiar with common ways to measure utilization of standard computer resources, such as CPU, memory, and bandwidth usage. As one example, all POSITAs would be familiar with the general functionality of standard Microsoft Windows operating systems. Windows Vista was a computer operating system that was available to the public by 2007. Windows Vista was a Microsoft Windows operating system that preceded Windows 8, which the '614 Patent admits was released for general availability in October 2012. See Ex. 1 at 7:20-27; Ex. 3 ¶ 97.

Windows Vista included (as did prior Windows operating systems and as have later Windows operating systems) an application—called “Windows

Task Manager” in Windows Vista—that monitors running applications and processes, and assesses computer performance. One tab, the “Performance” tab, shows, among other things, CPU usage and memory usage, including the percentage of CPU and memory availability.⁸ Another tab, the “Networking” tab, shows, among other things, allowed the monitoring of network connection utilization and speed. *See* Ex. 3 ¶ 98.

Task Manager in Windows 8 also could monitor hardware resource utilization, including memory and CPU usage. Further, it showed the applications or programs that are run at startup of a computer, its impact on computer usage (such as Low, Medium, or High), its Status (Enabled or Disabled), and allows the user to disable the application if its impact on resource usage is too great.⁹ *See* Ex. 3 ¶ 99.

Similarly, the Windows Server 2008 R2 operating system was available to the public in 2009. It preceded the Windows Server 2012 operating system that the '614 Patent admits was released in 2012. Ex. 1 at 6:30-42. Included in Windows Server 2008 R2 was Resource Monitor, showing hardware (such as CPU and memory) utilization. It also monitored network congestion and TCP connections, and showed whether any net-

⁸ A high level overview of Windows Vista Task Manager, which identifies a subset of the knowledge that would be possessed by a POSITA, is found at <https://www.techrepublic.com/article/windows-vistas-task-manager-the-harder-to-detect-changes/> (Ex. 24). Further information regarding a POSITA's knowledge of Windows Vista Task Manager is contained in *Introducing Microsoft Windows Vista 8.1*, William R. Stanek (2006).

⁹ A high-level overview of Windows 8 Task Manager, which identifies a subset of the knowledge that would be possessed by a POSITA, is found at <https://blogs.windows.com/windowsexperience/2013/06/06/windows-8-task-manager-in-depth/> (Ex. 25).

work adapters or IP addresses had network congestion issues.¹⁰ See Ex. 3 ¶ 100.

Not only would a POSITA have been familiar with the task management functionality of the operating systems discussed above, a POSITA would have been familiar with these and other common operating systems, including Microsoft Windows and Linux operating systems. The Linux operating system was first released in 1991, with many different distributions released between then and 2013. The Linux operating system adopted the process abstraction of UNIX-based systems, developed starting in the late 1960s, and like UNIX, included a number of mechanisms and tools for monitoring, measuring, and understanding resource consumption (*e.g.*, the “top” shell command, the “ps” shell command, the “/proc” file system, etc.). Further, Windows XP and Windows 7 (both listed in Claim 10 of the Patent) were released in 2001 and 2009, respectively, with other versions of the Windows operating system (*e.g.*, Windows 95) being released even earlier. See Ex. 3 ¶ 101.

4.11. Background Prior Art

4.11.1. Squid (Ex. 13)

The book Squid, by Wessels (Ex. 13), is a well-known reference work on the implementation of a widely used open source proxy server. See Ex. 3 ¶ 102.

The Squid book was published in January of 2004 by O'Reilly Media (ISBN-10: 9780596001629, ISBN-13: 978-0596001629), and thus quali-

¹⁰ A high-level overview of Windows Server 2008 R2 Resource Monitor, which identifies a subset of the knowledge that would be possessed by a POSITA, is found at <https://www.techrepublic.com/blog/the-enterprise-cloud/use-resource-monitor-to-monitor-network-performance/> (Ex. 26).

fies as prior art under 35 U.S.C. § 102(a)(1). Squid has been cited in other U.S. patents and thus was publicly available from this date. *See, e.g.*, U.S. Pat. Nos. 8,725,730 (cited by applicant), 10,805,429 (citation by patent owner of '614 patent, in a related patent).

4.11.2. Luotonen (Ex. 14)

Web Proxy Servers is a book authored by Ari Luotonen that was published in 1998 (ISBN-10: 0136806120). It therefore qualifies as prior art under 35 U.S.C. § 102(a)(1). Luotonen has been cited in other U.S. patents and thus was publicly available from this date. *See, e.g.*, U.S. Pat. Nos. 6,651,103 (cited by applicant), 10,805,429 (citation by patent owner of '614 patent, in a related patent).

4.11.3. Fogel (Ex. 35)

“Modeling the Human Operator with Finite-State Machines” is a NASA Contractor Report by L.J. Fogel and Roger A. Moore that was published in July 1968. It therefore qualifies as prior art under 35 U.S.C. § 102(a)(1). Fogel is cited herein as background prior art pertinent to construing the claim language concerning the “state” of a device, and “shifting state.” Fogel demonstrates the broad application of finite state machines, such as to represent the human operator in the performance of flight control (a complex subject), and simplifying the analysis by modelling the human subject as having distinct internal “states,” with rules as to associating transitions between the distinct states with specific inputs. *See* Ex. 35 at 1 (Summary).

4.12. Applicant Admitted Prior Art (AAPA)

The specification includes the commonly seen disclaimer that matter in the Background section is not admitted to be prior art. *See* Ex. 1 1:27-30. On the other hand, there are statements in the Background section of the '614 patent that do specifically refer to the disclosures therein as "prior art." *See, e.g.,* Ex. 1 3:66-4:31, 28:15-29-3, 79:64-65 (referring to Fig. 52), 80:15-20 (referring to Figs. 36a, 36b, and 37), 81:10-19 (referring to Figs. 58, 60, and 61), 103:5-23, 149:51-52, 150:36-56, 151:1-152-10, 153:33-57, and Figs. 1, 2, 3a, 4, and 4a.

In any case, as the BPAI ruled in *Ex parte Shirley* (Appeal 2009-2352), despite disclaimers to the contrary, when the specification as a whole implies that a particular statement reflects the applicant's view of the prior art, then the Examiner has a *prima facie* case for the statement being AAPA.

In this regard, most of the first 50 columns of the '614 patent constitute a far-ranging discussion of the core technologies of the Internet as of the 2013 filing date, including a broad survey and explanation of network-based data transmission technologies, with considerable documentation of supporting references, including the RFCs and industry standards referenced herein. The applicant's statements in this patent about this extensive background constitute strong additional reasons to accept the RFCs and standards referenced therein as printed publication prior art, and further, absent intrinsic indications to the contrary, to accept the admissions on the face of the '614 patent as acknowledgement that the subject matter of those statements is prior art in and of themselves.

5. SUMMARY OF SNQs/PROPOSED REJECTIONS AND WHY THEY RAISE SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

The substantial new questions of patentability presented in this request fall into three groups, based primarily on the Shribman '733 publication, Mithyantha, and MorphMix, respectively. These SNQs are as follows:

5.1. SNQ I—Grounds based primarily on the Shribman '733 publication

SNQ Ia: Claims 1, 3-5, 7-9, 13, 17, 25-26, and 29 are anticipated by the Shribman '733 Publication under 35 U.S.C. § 102(a)(1).

Why SNQ Ia presents a substantial new question of patentability.

SNQ Ia presents a substantial new question of patentability because it is based on the Shribman '733 publication, which was not applied by the Examiner or addressed in substance on the record by either the Examiner of the Applicant in the original examination of the '614 patent. The reasons that Requester believes the Shribman '733 publication avoided more thorough review are set forth in Section 3.5 above, concerning the prosecution history. The Shribman '733 publication generally discloses deploying a geographically diverse array of peer devices that can interchangeably function as clients, peers, or agents (caching proxies), which is distinct from the disclosure of any other reference considered or discussed during the original examination. Therefore, the Shribman '733 publication constitutes a “new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the ['614] patent for which reexamination is requested.” MPEP § 2216.

SNQ Ib: Claims 1-5, 7-9, 13, 17, 25-26, and 29 are obvious under 35 U.S.C. § 103(a) over the Shribman '733 Publication in view of Liu.

Why SNQ Ib presents a substantial new question of patentability.

SNQ Ib presents a substantial new question of patentability because it is based on the combination of (1) the Shribman '733 publication, which was neither applied nor addressed in the original examination of the '614 patent, as explained above and (2) Liu, which was not before the Examiner in the original examination in any capacity. Liu generally discloses the detection and prevention of denial of service attacks in dynamic distributed systems and an information layer agent that determines if events indicate attacks, which is distinct from the disclosure of any other reference considered or discussed during the original examination. Therefore, Liu also constitutes a “new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the ['614] patent for which reexamination is requested.” MPEP § 2216.

SNQ Ic: Claim 2-6, 8-10, 14-27, and 29 is obvious under 35 U.S.C. § 103(a) over the Shribman '733 Publication in view of Sigurdsson and/or Chauhan.

Why SNQ Ic presents a substantial new question of patentability.

SNQ Ic presents a substantial new question of patentability because it is based on the combination of (1) the Shribman '733 publication, which was neither applied nor addressed in the original examination of the '614 patent, as explained above and (2) Sigurdsson and/or Chauhan. Although Sigurdsson and Chauhan were cited and applied in the original examination, they were only cited with regard to the claim steps concerning the periodic or continuous tracking of “state” of the client device (steps [1.1]-

[1.6]], and not in combination with a reference such as the Shribman '733 publication, which clearly the other aspects of issued claim 1, concerning performing the performance of the specified content retrieval task by an available client device (steps [1.7-1.11]). The Examiner did not withdraw his findings as to Sigurdsson and Chauhan, but, as addressed in the Examiner's reasons for allowance, the Examiner was unable to cite prior art addressing the further combination with the claimed content retrieval task. *See* Ex. 2 at 22-23. The addition of the Shribman '733 publication changes this analysis, in that the "state" tracking aspects remain disclosed as before by Sigurdsson and Chauhan, whereas the content retrieval aspects are fully disclosed by the Shribman '733 publication, with a clear motivation to combine, as reflected by the steps disclosed in the Shribman '733 publication itself to track the state of the client devices.

SNQ Id: Claims 2-6, 8-10, 14-27, and 29 is obvious under 35 U.S.C. § 103(a) over the Shribman '733 publication in view of Liu and in further view of Sigurdsson and/or Chauhan.

Why SNQ Id presents a substantial new question of patentability.

SNQ Id presents a substantial new question of patentability because it is based on the combination of (1) the Shribman '733 publication, which was neither applied nor addressed in the original examination of the '614 patent, as explained above, (2) Liu, which was not before the Examiner in the original examination in any capacity, as explained above, and (3) Sigurdsson and/or Chauhan, both of which were cited and applied in the original examination (though on a more limited basis as discussed above).

SNQ Ie: Claims 11-12 is obvious under 35 U.S.C. § 103(a) over the Shribman '733 Publication in view of Bhatia.

Why SNQ Ie presents a substantial new question of patentability.

SNQ Ie presents a substantial new question of patentability because it is based on the combination of (1) the Shribman '733 publication, which was neither applied nor addressed in the original examination of the '614 patent, as explained above and (2) Bhatia (which was cited and applied in the original examination, as to claims 11-12).

SNQ If: Claims 11-12 are obvious under 35 U.S.C. § 103(a) over the Shribman '733 Publication in view of Liu and in further view of Bhatia.

Why SNQ If presents a substantial new question of patentability.

SNQ If presents a substantial new question of patentability because it is based on the combination of (1) the Shribman '733 publication, which was neither applied nor addressed in the original examination of the '614 patent, as explained above, (2) Liu, which was not before the Examiner in the original examination in any capacity, as explained above, and (3) Bhatia, which was cited and applied in the original examination as to claims 11-12.

SNQ Ig: Claim 28 is obvious under 35 U.S.C. § 103(a) over the Shribman '733 publication in view of Ebata.

Why SNQ Ig presents a substantial new question of patentability.

SNQ Ig presents a substantial new question of patentability because it is based on the combination of (1) the Shribman '733 publication, which was neither applied nor addressed in the original examination of the '614 patent, as explained above and (2) Ebata, which was not before the Examiner in the original examination in any capacity. Ebata generally discloses the selection of proxies based on, *inter alia*, their geographic location, which is distinct from the disclosure of any other reference considered or discussed during the original examination. Therefore, Ebata also

constitutes a “new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the [’614] patent for which reexamination is requested.” MPEP § 2216.

SNQ Ih: Claim 28 is obvious under 35 U.S.C. § 103(a) over the Shribman ’733 publication in view of Liu and in further view of Ebata.

Why SNQ Ih presents a substantial new question of patentability.

SNQ Ih presents a substantial new question of patentability because it is based on the combination of (1) the Shribman ’733 publication, which was neither applied nor addressed in the original examination of the ’614 patent, as explained above, (2) Liu, which was not before the Examiner in the original examination in any capacity, as explained above, and (3) Ebata, which similarly was not before the Examiner in the original examination in any capacity, as explained above.

5.2. SNQ II—Grounds based primarily on Mithyantha

SNQ IIa: Claims 1-2, 4-12, 15-23, 25-26, and 29 are anticipated by Mithyantha under 35 U.S.C. § 102(a)(2).

Why SNQ IIa presents a substantial new question of patentability.

SNQ IIa presents a substantial new question of patentability because it is based on Mithyantha, which was not before the Examiner in the original examination of the ’614 patent in any capacity. Mithyantha generally discloses distributing network traffic over a plurality of devices which may be interconnected, where some of the devices may be regarded as clients, and others of which may be regarded as servers, depending on the role that the respective devices are assigned to play in the traffic distribution scheme, which is distinct from the disclosure of any other reference considered or discussed during the original examination. Therefore, Mithyantha consti-

tutes a “new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the [’614] patent for which reexamination is requested.” MPEP § 2216.

SNQ Iib: Claims 1-2, 4-12, 15-26, and 28-29 are obvious under 35 U.S.C. § 103(a) over Mithyantha in view of Internet Standards, Standard Practices for Application Startup Configuration, and the General Knowledge of a POSITA.

Why SNQ Iib presents a substantial new question of patentability.

SNQ Iib presents a substantial new question of patentability because it is based on the combination of (1) Mithyantha, which was not before the Examiner in the original examination of the ’614 patent in any capacity, as explained above, (2) internet standards, and (3) standard practices for application startup configuration and the general knowledge of a POSITA. With respect to internet standards, RFC 2616, a definitive specification for the HTTP/1.1 protocol, is discussed in the ’614 patent specification (Ex. 1, 5:1 and 5:63, and was submitted in an IDS during prosecution of the ’614 patent (Ex. 2 at 571 and 573, but the prosecution history does not reflect that RFC 2616 was addressed by the applicant or applied by the Examiner in the original examination of the claims. RFC 791, a specification for the IP protocol (“Internet Protocol”) that as its name implies underlies the entire Internet, and RFC 793, for TCP, a connection-oriented end-to-end protocol using IP packets as specified in RFC 791, are foundational to the entire Internet. These standards were also cited in an IDS (Ex. 2 at 571) and mentioned in the ’614 specification (Ex. 1, 1:57, 3:37), but were not addressed by the applicant or mentioned or applied by the Examiner in the original examination. Similarly, with respect to standard

practices for application startup configuration and the general knowledge of a POSITA, the standard practices for application startup configuration and the general knowledge of a POSITA, including common ways to measure utilization of standard computer resources, such as CPU, memory, and bandwidth usage, in well-known and generally available operating systems, were not cited to or by the Examiner in the original examination, or otherwise considered on the record. While the Examiner may have been generally aware of such subject matter in and of itself, he did not have Mithyantha before him and thus was not in a position to have addressed any such combination of Mithyantha with such further teachings. Therefore, the new reference, Mithyantha, when viewed in light of internet standards, standard practices for application startup configuration, and the general knowledge of a POSITA, constitute “new, non-cumulative technological teaching[s] that w[ere] not previously considered and discussed on the record during the prosecution of the application that resulted in the [’614] patent for which reexamination is requested.” MPEP § 2216.

5.3. SNQ III—Grounds based primarily on MorphMix

SNQ III: Claims 1-2, 4-5, 7-10, 13, 17-26, and 29 are obvious under 35 U.S.C. § 103(a) over MorphMix in view of Standard Practices for Application Startup Configuration and the General Knowledge of a POSITA.

Why SNQ III presents a substantial new question of patentability.

SNQ III presents a substantial new question of patentability because it is based on the combination of (1) MorphMix, which was not before the Examiner in the original examination of the ’614 patent in any capacity, (2) standard practices for application startup configuration and the general knowledge of a POSITA, which was not cited to, cited by, or ap-

plied by the Examiner in the original examination, as explained above. MorphMix generally discloses a peer-to-peer-based system for anonymous internet access, which is distinct from the disclosure of any other reference considered or discussed during the original examination. Therefore, MorphMix, in view of the further teachings of standard practices for application startup configuration, and the general knowledge of a POSITA, constitutes a “new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the [’614] patent for which reexamination is requested.” MPEP § 2216.

6. PERTINENCE AND MANNER OF APPLYING THE PRIOR ART

The following standards and considerations are applied herein with respect to the particular proposed grounds for rejection set forth in Sections 7-9 below.

6.1. Legal Standards

6.1.1. Standard for Anticipation

A claim is anticipated if “each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” MPEP 2131, citing *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). To reject a claim as anticipated by a reference, the disclosure must teach every element required by the claim under its broadest reasonable interpretation. MPEP 2131.

As recently expressed by the Federal Circuit, to be anticipating, (1) “a prior art reference must disclose all elements of the claim within the four corners of the document, and it must disclose those elements arranged as in the claim,” or (2) “if [the reference] does not expressly spell out all the limitations arranged or combined as in the claim,” it can still anticipate “if a person of skill in the art, reading the reference, would at once envisage the claimed arrangement or combination.” *Microsoft Corp. v. Biscotti, Inc.*, 878 F.3d 1052 (Fed. Cir. 2017).

Inherency—*Microsoft Corp. v. Biscotti* above reflects the possibility of inherent anticipation. Under the doctrine of inherency, if an element is not expressly disclosed in a prior art reference, the reference will still be deemed to anticipate a subsequent claim if the missing element “is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill.” *Cont’l Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1268 (Fed. Cir. 1991). *See also* MPEP 2112.

According to *Cont’l Can*, “[t]o serve as an anticipation when the reference is silent about the asserted inherent characteristic, such gap in the reference may be filled with recourse to extrinsic evidence.” *Id.* The *Cont’l Can* decision continues: “Such evidence must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill . . . [i]f . . . the disclosure is sufficient to show that the natural result flowing from the operation as taught would result in the performance of the questioned function, it seems to be well settled that the disclosure should be regarded as sufficient.” *Id.* Distinguishing this rationale from an obviousness determination under § 103, the court went on to state: “This modest flexibility in the rule that ‘anticipation’ requires that every element

of the claims appear in a single reference accommodates situations where the common knowledge of technologists is not recorded in the reference; that is, where technological facts are known to those in the field of the invention, albeit not known to judges.” *Id.*

Computer-Implemented Inventions Claimed in Functional Terms; Genus-Species; Disclosure of a Species Anticipates the Genus—Where elements of a claim are broadly specified in functional terms, such that the claim is not limited to a specific structure, and purports to cover all devices that are capable of performing the recited function, prior art that “discloses a device that can inherently perform the claimed function” may be an appropriate basis for rejection under 35 U.S.C. § 102 and/or 35 U.S.C. § 103. MPEP 2114, Subsection IV (Computer-implemented functional claims). This analysis is also reflected in the rules applicable to genus/species situations, *e.g.*, as addressed in MPEP 2131.02.

The claims at issue here concern interconnected nodes in a network. Claim 1 addresses these connections at the highest level, in functional terms, wherein connections between two nodes may be through one or more other nodes, the same devices performing the roles of the certain nodes are also capable of performing the roles of other types of nodes, and so forth. The broadest claims here are for *generic* constructs, with features that are general in the sense that, in any given embodiment, they can be substituted by more specific structures (species) and still be within the scope of the claim. Claim 1 in this case is to a *genus*, comprising many *species* that may be found to be within the claim.

For example, the '614 specification discloses embodiments in which the clients that can act as proxies under the control of the acceleration server are part of a larger peer group, in which they can also be clients

seeking their own content retrieval with the assistance of the acceleration server. This further topology, however, is simply a species of the possible network layouts that fall under claim 1. Other species may not require that the recited client device also happens to be a client *of the first server*.

The claims also recite a “server” that tracks the state of other devices. While one possibility is that this server is the Acceleration Server 32 in Fig. 5 of the ’614 patent, the disclosure of the patent is far more general: *any* of the disclosed devices can track *any* of the others, and *any* of the disclosed devices may be tracked. See Ex. 1 at 122:24-126:11. This opens many possibilities of how the devices shown in the figures of the ’614 patent may be mapped to its claims, and this is not by any means limited to the most straightforward mapping. The claims as written clearly cover more than a single topology.

Claim 1 of the ’614 patent is thus generic in the sense that it covers a range of different embodiments. Some of this range of possible embodiment are reflected, for example, in a number of the dependent claims. Therefore, because disclosure of *any single species* falling within the scope of a broader generic claim *always* anticipates the genus, disclosure in the prior art of any specific embodiment of the generic architecture identified in claim 1 would render it anticipated and/or obvious. MPEP 2131.02.¹¹

¹¹ See also *In re Slayter*, 276 F.2d 408, 411 (CCPA 1960) (broad claim to a fiber-reinforced composite ceramic structure where the fiber and fused ceramic differ in modulus of elasticity anticipated by earlier disclosure of a glass structure with embedded metal fibers; “It is well settled that a generic claim cannot be allowed to an applicant if the prior art discloses a species falling within the claimed genus; in other words, whatever would infringe if subsequent will anticipate if prior.”).

6.1.2. Standard for Obviousness

A conclusion of obviousness is appropriate “if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains.” 35 U.S.C. § 103. This determination requires the Board to consider (1) the scope and content of the prior art, (2) the differences between the claimed invention and the prior art, and (3) the level of ordinary skill in the pertinent art. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18. Secondary considerations, such as commercial success, long felt but unsolved needs, failure of others, etc., can also be considered, where applicable, to counter a *prima facie* showing of obviousness. See *id.* “The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.” *KSR Int’l v. Teleflex, Inc.*, 550 U.S. 398, 417 (2007). “If a person of ordinary skill can implement a predictable variation, § 103 likely bars its patentability.” *Id.*

Inherency vs. Obviousness. The Examiner will note that in some cases this Request presents arguments as to the same claims both as a matter of inherent anticipation, as well as obviousness.

Obviousness is not at all inconsistent with inherent disclosure. See MPEP 2112(III); *In re Best*, 562 F.2d 1252, 1255 n.4, 195 USPQ 430, 433 n.4 (CCPA 1977) (“There is nothing inconsistent in concurrent rejections for obviousness under 35 U.S.C. 103 and for anticipation under 35 U.S.C. 102”).

The difference between inherent anticipation and obviousness grounds is as follows.

In the case of inherent disclosure of a claim feature, the argument (as already reviewed above) is that what is expressly disclosed in the prior art necessarily must also include the specified feature, even if that feature is not expressly noted as such in the disclosure. In the case of obviousness, the argument is *not* that the feature necessarily must be present, but rather, that, in any case, even if not necessarily present, it would have been obvious to a POSITA to have included it.

As noted in MPEP 2112(III) cited above, inherency and obviousness are not mutually exclusive or inconsistent. The Examiner does not have to elect one approach or the other. Where supported by the facts, the Examiner, in rejecting a claim, is fully entitled to rely on *both* inherent anticipation under 35 U.S.C. § 102 *and* obviousness under 35 U.S.C. § 103.

Alternative Limitations. Many of the claims of the '614 patent recite limitations in the alternative, in the form of “A method comprising [A] and [B].” Such claims are anticipated by a disclosure of either one of [A] or [B]. MPEP 2131 (“When a claim covers several structures or compositions, either generically or as alternatives, the claim is deemed anticipated if any of the structures or compositions within the scope of the claim is known in the prior art.”) (citing *Brown v. 3M*, 265 F.3d 1349, 1351 (Fed. Cir. 2001)).

6.2. Level of Skill in the Art

Graham v. John Deere Co. also states that an obviousness analysis must take into account the level of skill in the art. 35 U.S.C. § 103 directs that the pertinent level of skill for assessing obviousness is the level of skill possessed by a person of ordinary skill (POSITA) in the the field of the claimed invention, as of the time of the claimed invention.

The '614 patent, under the heading “Technical Field,” states that it “relates generally to an apparatus and method for improving communication over the Internet by using intermediate nodes, and in particular, to using devices that may doubly function as an end-user and as an intermediate node.” Ex. 1 at 1:19-23. This field may generally be described as the field of Internet communications.

According to the accompanying expert opinion of Keith J. Teruya (Ex. 3), a person of ordinary skill in the art (“POSITA”) in the field of Internet communications in the 2013 timeframe of the claimed invention would have had (1) at least a bachelor’s degree or equivalent in a field such as Electrical Engineering, Computer Engineering, or Computer Science, or an equivalent field that includes network engineering as a topic of study, plus at least one year of practical academic or industry technical experience in the computer network field, such as serving as an engineer for an Internet service provider performing network design, development, or configuration tasks, or as a software developer for network communications software or related utility software, and would be familiar with the underlying principles of Web, Internet, and network communication, data transfer, and content sharing across networks, including the HTTP and TCP/IP protocols, and the pertinent Internet RFCs, or (2) at least three years’ full-time technical experience as stated (or an equivalent combination of academic study and work experience). See Teruya Decl., Ex. 3 ¶¶ 18-20.

6.3. Analogous Nature of The Cited Prior Art

“[A] reference is analogous art to the claimed invention if: (1) the reference is from the same field of endeavor as the claimed invention (even if it addresses a different problem); or (2) the reference is reasonably pertinent

to the problem faced by the inventor (even if it is not in the same field of endeavor as the claimed invention).” MPEP 2141.01(a)(I), citing *In re Bigio*, 381 F.3d 1320, 1325, 72 USPQ2d 1209, 1212 (Fed. Cir. 2004).

As reflected in the Examiner’s field of search (709/217, 218, 219, 232, 235), the ’614 patent is generally in the field of transferring data among multiple computers, over interconnected networks (Internet), from a remote server, regulating the data transfer, and avoiding congestion.

The references applied herein are all in this field. Other references cited as background art are reference works broadly addressing the field (*e.g.*, Squid (Ex. 13), Luotonen (Ex. 14) or pertinent to solving problems arising in connection with the claimed implementation (*e.g.*, Fogel (Ex. 35), GOF (Ex. 27), Windows documentation concerning task management, resource monitoring, and startup (Exs. 24, 25, and 26).

The **Shribman ’733 publication** (Ex. 6), an earlier publication by the same inventors, addresses the same objects as the ’614 patent, that of providing the services of multiple intermediate devices for Internet content retrieval, in a peer-to-peer arrangement. It pursues the same ends, which is to achieve Internet content retrieval acceleration by using an array of peer devices, being just an earlier iteration of the effort. The provisional of the ’614 patent, in fact states that the disclosure was “[a] different way to implement the acceleration system described in hola’s [the Patent Owner’s predecessor’s] patent application 12836059 [the serial number of the application published in the Shribman ’733 publication].” Ex. 5 at 125. The Shribman ’733 publication is thus acknowledged in the family of the ’614 patent as its predecessor, a different way to solve the same problem. The statements in the provisional of the ’614 application, as well as the references throughout the ’614 patent to ’604 patent that eventuated from the

Shribman '733 publication (and the incorporation of the entire '604 patent by reference (*see* Ex. 1, 31:53-67)), the make clear that the inventors regarded their prior application published as the Shribman 733 publication to be the direct predecessor of the '614 patent herein under consideration. As such, the Shribman '733 publication is clearly analogous.

Mithyantha (Ex. 10), like the '614 patent, is also directed at an effort to improve communication over the Internet by using intermediate nodes. More particularly, it relates to deployment of network appliances to be used as intermediate communications nodes to improve network communications. *See, e.g.*, Ex. 10 at Abstract, 5:31-8:35. It addresses a “cluster” of appliances, similar to the plurality of peer devices in the '614 patent, to achieve “performance gains” in data retrieval. Ex. 10, 51:31-48. Among other features, analogous to the acceleration server of the '614 patent, the appliances in Mithyantha provide “acceleration services.” *Id.*, 23:48-55.

Moreover, the appliances disclosed in Mithyantha have dual functionality, like the clients/tunnel devices of the '614 patent:

In some embodiments, a client 102 has the capacity to function as both a client node seeking access to applications on a server and as an application server providing access to hosted applications for other clients 102 a-102 n.

Id. at 6:31-35. Mithyantha thus uses similar devices in similar combinations to similar ends, including the same objective of accelerating content retrieval over the Internet using a cluster of peer devices, and is likewise analogous art.

MorphMix (Ex. 11) concerns achieving anonymity for Internet users. Achieving anonymity for Internet users is also one of the objects of the '614 patent, *see* Ex. 1 at 42:48-43:12, 52:8-19. Morphmix provides anonymity by directing the user's communications through a plurality of intermediate

devices, much like the plurality of peers and agents deployed in the '614 patent. Thus, the MorphMix reference presented in this Request teaches precisely the benefit of using many ordinary computers as proxies to send anonymous web requests on behalf of others. Also like the '614 patent, any user's computer in the arrangement may also serve as an intermediate retrieval node. MorphMix is thus yet another peer-to-peer Internet content retrieval implementation, with both objects and implementation similar to that of the '614 patent, and highly analogous.

Liu (Ex. 29) concerns the detection and prevention of denial of service attacks in dynamic distributed systems, such as those described in the '614 patent, including peer-to-peer (P2P) environments, mobile networks, and grid computing environments. *See* Ex. 29 ¶ [0027]. Like the '614 patent, Liu, even if it addresses the protection of general computational “nodes,” nevertheless describes the analogous problem of managing a plurality of deployed devices over the Internet, and providing a management overlay that tracks the state of nodes deployed on the Internet, including by “detect[ing] a change of state (*e.g.*, a transition from “medium-high” CP usage to “high” CPU usage), a threshold value that is reached, or a threshold rate of change that is reached (*e.g.*, in the case of a sudden, rather than an incremental change in resource usage is detected).” Ex. 29 ¶ [0058]. The solution provided by Liu for tracking these states, internally on the deployed device, for determining outside the device how to deal with the nodes, depending on their state, is directly analogous to the state tracking and transitions of Fig. 30 of the '614 patent. The implementation of this feature as disclosed in Liu would have commended itself to a POSITA seeking to implement a like monitoring function in a distributed information retrieval setting (such as what was envisioned in the '614 patent) to make

sure (as in Liu) that resources to be selected to perform retrieval are in an appropriate operational state. Ex. 3 ¶¶ 116-17.

Sigurdsson (Ex. 7), assigned to Google LLC, concerns the problem of synchronizing files between a user client and a peer client, in-place, that is, without having to move the files to a special synchronization folder, involving exchanging metadata “if the peer client and the first client are currently operating and visible to each other on a network.” *See, e.g.* Ex. 7 at Abstract. The reference is in the general field of data communications among multiple computers over the Internet, and more particularly is directly pertinent to keeping track of which peers are online and available, as addressed in the claims of the ’614 patent. Sigurdsson’s disclosed methods of tracking the available bandwidth of a connection to a peer (¶ [0008]) and online status of a peer by “monitoring polling” (¶ [0061]) would have commended itself to a POSITA seeking to implement a mechanism to ensure that content retrieval agents were similarly available for the task of retrieving content from a remote source. Sigurdsson is analogous art.

Chauhan (Ex. 8), like Mithyantha and Jackowski, with which (as noted above it shares some overlapping disclosure), relates to deployment of network appliances to be used as intermediate communications nodes to improve network communications, in this case by establishing standing routes over the appliances, between clients and servers. *See* Ex. 8 at Abstract, ¶ [0201]. The reference is thus in the general field of data communications among multiple computers over the Internet. Moreover, Chauhan also teaches techniques for tracking when the intermediate node devices (appliances) are available to the clients, which is directly pertinent to the same problem as addressed in the ’614 patent, in a highly similar technical context of communicating through intermediate devices, which would

have commended itself to a POSITA to solve the corresponding problem in the context of the '614 patent.

Jackowski (Ex. 9), like Mithyantha and Chauhan, with which (as noted above it shares some overlapping disclosure), relates to deployment of network appliances to be used as intermediate communications nodes to improve network communications, in this case including routing through peer tunnels. *See* Ex. 9 at Abstract. The reference is thus in the general field of data communications among multiple computers over the Internet. Moreover, Jackowski also teaches state transitions based on availability of the peer devices, and the further feature of the device accepting a task based on being in a first state (Ex. 9 ¶¶ [0220]-[0221]), which is directly pertinent to the same problem as addressed in the '614 patent, in a highly similar technical context of communicating through intermediate devices, which would have commended itself to a POSITA to solve the corresponding problem in the context of the '614 patent.

RFCs 2616, 791, 793 (Exs. 12, 22, and 28) are key Internet standards.

RFC 2616 is the then current specification for the HTTP protocol underlying the Worldwide Web, and thus the principal standard for the environment in which the '614 patent operates. RFC 2616 is cited in the '614 patent as having “standardized” the HTTP 1.1 protocol (Ex. 1, 4:62-5:9, 5:62-64), and thus would have been highly pertinent (indeed necessary) knowledge for a POSITA seeking to implement a like solution.

RFCs 791 and 793 define the IP and TCP protocols, respectively, both foundational technologies of the Internet. Ex. 3 ¶ 122. IP is referred to in the '614 patent as the “dominant protocol of the Internet.” Ex. 1 at 3:35-

39. Likewise, the '614 specification refers to TCP as defined by RFC 793 as “one of the core protocols of this Internet.” *Id.* at 2:54-60.

RFCs 791 and 793 (as well as RFC 2616) are analogous because they are pertinent to any invention that purports to be “for improving communication over the Internet” as stated in the '614 patent (Ex. 1 at 1:19-21). They are pertinent because knowledge of such standards is required in order to make useful contributions to how such communications work, and persons seeking to implement such solutions would want their solutions to be standards compliant. Knowledge of the standards is also necessary to interoperate with the Internet infrastructure in which the subject systems are completely enveloped, and on which they critically depend. Ex. 3 ¶ 123.

Squid (Ex. 13) is a well-known reference book on proxy technology in general and pertinent to any deployment of proxy devices, as well as to managing deployments involving multiple such devices. The '614 patent (Ex. 1 describes proxy functionality at 27:14-43 and states that it incorporates proxy functionality at 83:4-10. The Squid book, as a general treatise on Internet proxy servers, which concerns content retrieval through an intermediate agent, as in the '614 patent, is clearly pertinent to the problems being addressed in the '614 patent.

Dorso (Ex. 16) concerns peer-to-peer content retrieval through multiple peers and is clearly analogous, where the subject '614 patent states that it is in the field of “improving communication over the Internet by using intermediate nodes.” Ex. 1 at 1:19-21.

Bhatia (Ex. 17) concerns using mobile devices for data communications over the Internet and is directly pertinent to the claims concerning implementation of the '614 patent's client devices as mobile devices

running mobile operating systems. The '614 patent addresses the issue of improving Internet communications through mobile devices. Ex. 1 at 119:22-120:34. To the extent a POSITA would have any question whether the system of the '614 patent could have been implemented with mobile devices, Bhatia would have commended itself to the POSITA as showing how such deployments previously had been effectuated.

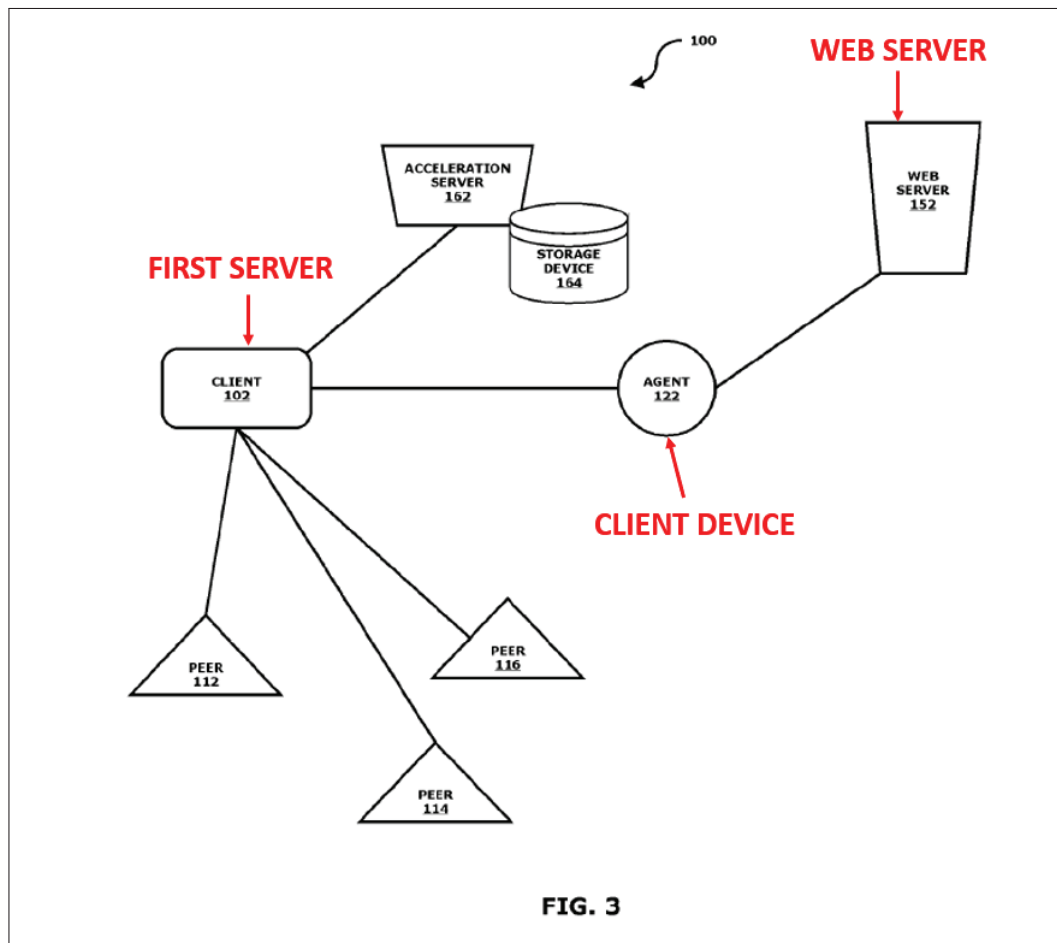
Ebata (Ex. 23) concerns an environment in which, like the '614 patent, users may retrieve content through a plurality of proxies, and wherein one of the criteria for selecting a proxy to use for the retrieval is the geographic location of proxy. *E.g.*, Ex. 23 at 4:34-47. The Ebata reference itself is analogous in its entirety, in terms of being in the same field as the '614 patent and addressing similar operational issues of selecting an optimal retrieval agent, and is directly pertinent to claim 28, in that Ebata prescribes the same solution of using the location of the available retrieval devices in order to make an appropriate selection.

7. SNQ I: ANTICIPATION AND/OR OBVIOUSNESS GROUNDS AS TO ALL CLAIMS, BASED ON THE SHRIBMAN '733 PUBLICATION

The Shribman '733 publication (Ex. 6) is an earlier publication in the same field by the same inventive entity as in the '614 patent.

The Shribman '733 publication, similar to the '614 patent, discloses “dual role” client devices—See Ex. 6 ¶ [0041] (“communication device 200 of FIG. 4 may serve as a client, agent, or peer”). A client device may thus serve in any of the capacities of client, agent, or peer. Thus, a “client device” also has a role, in the same embodiment, in which it acts as a proxy (agent) to retrieve web content for other like client devices.

The claims of the '614 patent may be mapped onto the disclosure of the Shribman '733 publication (as represented in this annotated version of Fig. 3 of Shribman), as follows:



Shribman Fig. 3, annotated

In the Shribman '733 publication, client devices 200 can act as both a client 102, or an agent 122 (as well as a peer 112). In that sense (at a minimum),¹² the device that serves as agent 122 also happens to be

¹² Requester notes that the '614 claims are broadly drafted, and that this is one mapping of elements consistent with the '614 claims and the Shribman '733 publication disclosure. As noted above, in raising a question as to the validity of a claim, it is sufficient to show that any one particular embodiment within the scope of the claim is anticipated or obvious. The

a client device acting as a client (running a web browser, etc.), and may be referred to as a “client device.” By the same token, the device that serves a client 102 also happens to be a client device having a dual role in the same embodiment as an agent, and thus a server, and may be regarded as the “first server” within the scope of claim 1. Moreover, as noted above in Section 3.6, the *Teso* court reaffirmed in its supplemental claim construction ruling (Ex. 30) that “a component can be *configured* to operate in different roles.” Ex. 30 at 10 (emphasis in original); *see also* Ex. 32 at 64 (instructing that Patent Owner’s expert could not testify “that a client device is specifically not a server”

There are two principal aspects of claim 1, which can be looked at in reverse order. Starting from the second half (“back end”) of the claim are the claim steps numbered herein as [1.7]-[1.11]:

* * *

[1.7] wherein the method is further configured for fetching over the Internet a first content identified by a first content identifier from a web server that is distinct from the first server, and the task comprising:

[1.8] receiving, by the client device, the first content identifier from the first server;

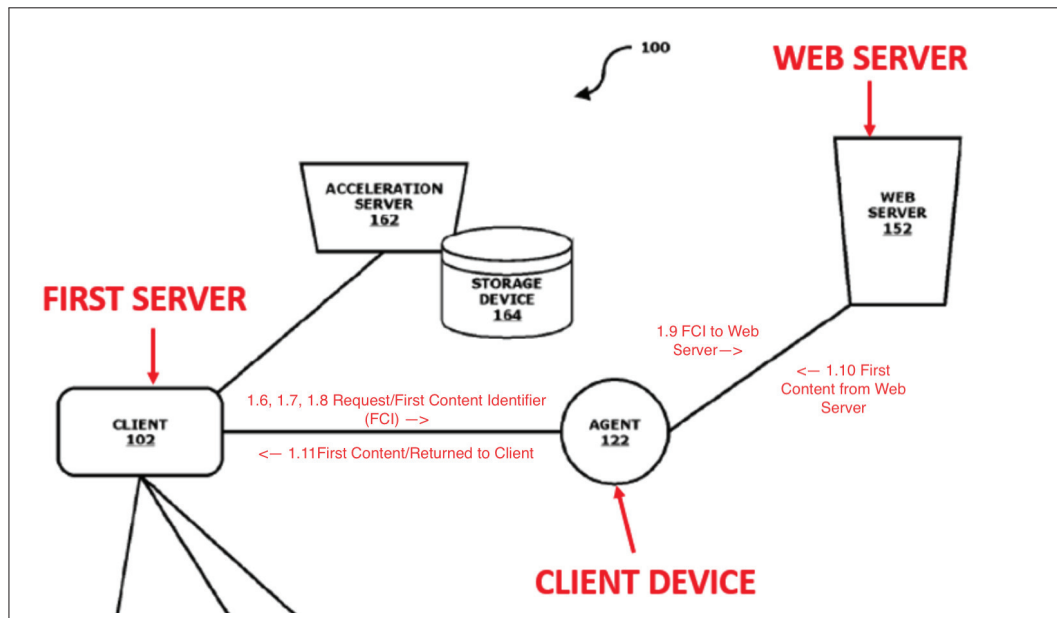
[1.9] sending, by the client device, the first content identifier to the web server;

[1.10] receiving, by the client device, the first content from the web server in response to the sending of the first content identifier; and

[1.11] sending, by the client device, the received first content to the first server.

These steps recite receiving, relaying, and returning a content request, which correspond to disclosure in the Shribman ’733 publication:

possible existence of other embodiments that may also be within the scope of the claim is of no consequence to this analysis.



Proxy Functionality in Fig. 3 of the Shribman '733 publication

The back end claim steps [1.7]-[1.11] read on the ordinary proxy retrieval of web content (where the agent 122 in Fig. 3 acts as the proxy), as detailed, for example, in well-known prior art such as the Luotonen and Squid references. *See, e.g.*, Ex. 13 at 1-2, 86; *see also* Ex. 3 ¶ 134.¹³ These steps of claim 1 constitute simple proxied content retrieval and are carried out identically as claimed, by agent 122 (client device) of the Shribman '733 publication, fetching content from web server 106.¹⁴ The “back-end” portion of the claim (steps [1.7]-[1.11]) is thus fully addressed by the Shribman '733 publication.

Turning now to the beginning part of the claim, these steps, the preamble [1.P] and the following claim steps [1.1]-[1.6] (“front end” steps), con-

¹³ Luotonen and Squid are cited as background prior art, basic Internet technology that any POSITA would be generally aware of by virtue of their training and/or experience.

¹⁴ As discussed in connection with step [1.7] below, the scenario and sequence of operations depicted in the above annotated diagram occurs in the circumstances addressed in ¶ [0089] of the Shribman '733 publication.

cern a mechanism based on a “state” determined by looking at the client device’s resource utilization, to verify that the client device is available to perform the content retrieval tasks recited in the “back end” claim steps [1.7]-[1.11]:

[1.P] A method for use with a resource associated with a criterion in a client device that communicates with a first server over the Internet, the client device is identified in the Internet using a first identifier and is associated with first and second state according to a utilization of the resource, the method comprising:

[1.1] initiating, by the client device, communication with the first server over the Internet in response to connecting to the Internet, the communication comprises sending, by the client device, the first identifier to the first server over the Internet;

[1.2] when connected to the Internet, periodically or continuously determining whether the resource utilization satisfies the criterion;

[1.3] responsive to the determining that the utilization of the resource satisfies the criterion, shifting to the first state or staying in the first state;

[1.4] responsive to the determining that the utilization of the resource does not satisfy the criterion, shifting to the second state or staying in the second state;

[1.5] responsive to being in the first state, receiving, by the client device, a request from the first server;

[1.6] performing a task, by the client device, in response to the receiving of the request from the first server,

* * *

This aspect is addressed in the Shribman ’733 publication as well. The Shribman inventors clearly considered the issue of agent availability in their ’733 publication, as reflected in the fact that the Shribman ’733 publication provides a “keep-alive” mechanism and corresponding database reflecting the “status” of agent and peer (client device) availability.

Based on the Examiner’s interpretation that “resource” includes collected available input and output capacities at the client device, and “state” includes some persistent record of the situation of the device based on previous inputs, it follows that the Shribman ’733 publication’s disclosure, of repeatedly checking the responsiveness of the device to keep-alive mes-

sages, and recording the result as a “status” of the device reflected in a database, is anticipating as to steps [1.1]-[1.6] of claim 1, and thus, together with the proxying features noted above (which the Shribman ’733 publication likewise fully discloses), anticipating as to claim 1 as a whole. This is the basis of the anticipation ground addressed in the following section.¹⁵

7.1. SNQ Ia/Anticipation of Claims 1, 3-5, 7-9, 13, 17, 25-26, and 29 by the Shribman ’733 Publication

7.1.1. SNQ Ia (§ 102-Shribman ’733 Publication)/Claim 1

Claim 1 recites a preamble (1.P) and limitations that Requester has numbered as 1.1-1.11.

1.P A method for use with a resource associated with a criterion in a client device that communicates with a first server over the Internet, the client device is identified in the Internet using a first identifier and is associated with first and second state according to a utilization of the resource, the method comprising:

As reflected in Fig. 3 of the Shribman ’733 publication, agent 122 (client device) communicates with client 102 (first server) over the Inter-

¹⁵ Indeed, the prior Examiner’s reasoning that Sigurdsson disclosed the limitations that now map to steps [1.2]-[1.4] of issued claim 1 (shifting state based on comparing resource utilization on the client device with a criterion) apply with the same force to the Shribman ’733 publication, which makes very similar disclosures in this regard. *Compare* Ex. 7 (Sigurdsson) ¶¶ [0008], [0061] and Fig. 8, ref. 804 *with* Ex. 6 (Shribman ’733 publication) ¶¶ [0069], [0099]. In the alternative to the ground presented here based on anticipation, the Examiner in reexamination could equally well find obviousness simply by combining the further disclosures of Shribman ’733 publication, including its disclosure of combining proxying with determining proxy availability based on resource utilization, with the prior grounds of rejection of original claim 1 set forth in the file wrapper. *See, e.g.*, Ex. 2 at 292-293.

net. The client device is identified in the Internet by an IP address (first identifier) Ex. 6 ¶ [0072].

The availability state of the client device is reflected in a database according to responses from “keep-alive” signals. Ex. 6 ¶¶ [0069] (connection status), [0099] (keep-alive monitoring).

Specifics of the publication’s disclosure of the “resource,” “criterion,” and first and second “states” referenced in the preamble are addressed below in connection with the claim steps that apply these terms. To the extent the preamble is deemed limiting, the Shribman ’733 publication discloses each of such requirements.

[1.1] initiating, by the client device, communication with the first server over the Internet in response to connecting to the Internet, the communication comprises sending, by the client device, the first identifier to the first server over the Internet;

Upon its own startup (and thus “in response to connecting to the Internet”), the agent 122 of the Shribman ’733 publication (client device), acting as a client, registers with acceleration server 162, sending its IP address (first identifier):

[0072] The initializer 222 is the first element of the communication device 200 to operate as the communication device 200 starts up (block 302). As the initializer 222 starts, it first communicates with the acceleration server 162 to sign up with the acceleration server 162. This is performed by providing the acceleration server 162 with the hostname, and all IP addresses and media access control (MAC) addresses of the interfaces on the communication device 200 having the initializer 222 thereon.

Ex. 6, Shribman ’733 publication, ¶ [0072].

This combination of events also constitutes initiating by the client device of communication *with the first server* over the Internet comprising

sending the first identifier to the first server. First, when a new client device goes online, the acceleration server shares a list of the origin IP addresses it will be handling with previously registered devices (which would include the device acting as the “first server” in these claims) (Ex. 6 ¶ [0066]), which a POSITA would understand as also identifying (by the IP address, which is the only available identifier) the device responsible for handling the new list being communicated. Ex. 3 ¶ 144. Additionally, the client device’s IP address is also sent by the acceleration server to client 102 (the first server) (Ex. 6, ¶ [0080]), and the IP address of the client device is reflected in the first server’s local “cache” database, see item 310 in Fig. 7. The client device thus initiates these communications, in response to connecting to the Internet, in which it sends its IP address to the first server. In either operation, the client device IP address is relayed through the acceleration server, but thereby “to” the first server as well. The net result in each case being of a process that begins on startup of the first client device, where it sends its IP address, by way of the acceleration server, to another client device that corresponds to the claimed “first server.” Requester submits that such relaying of information, initiated upon first connecting to the Internet (“as the communication device 200 starts up,” par. [0072]), is within the scope of “in response to connecting to the Internet,” under BRI. The language of claim step [1.1] should also not be read in a way that introduces a limitation (such as a limitation that the communication of the client device IP address on startup must be *directly* to the devices that operates as the first server), as to which there is no corresponding embodiment in the specification, which would be the case here.¹⁶

¹⁶ The supporting disclosure of the ’614 patent in this regard is substantially identical to the disclosure of the predecessor Shribman ’733 publication. Compare Shribman ’733 publication, Ex. 6 ¶¶ [0066] (startup)

The Shribman '733 publication thus discloses this limitation.

[1.2] when connected to the Internet, periodically or continuously determining whether the resource utilization satisfies the criterion;

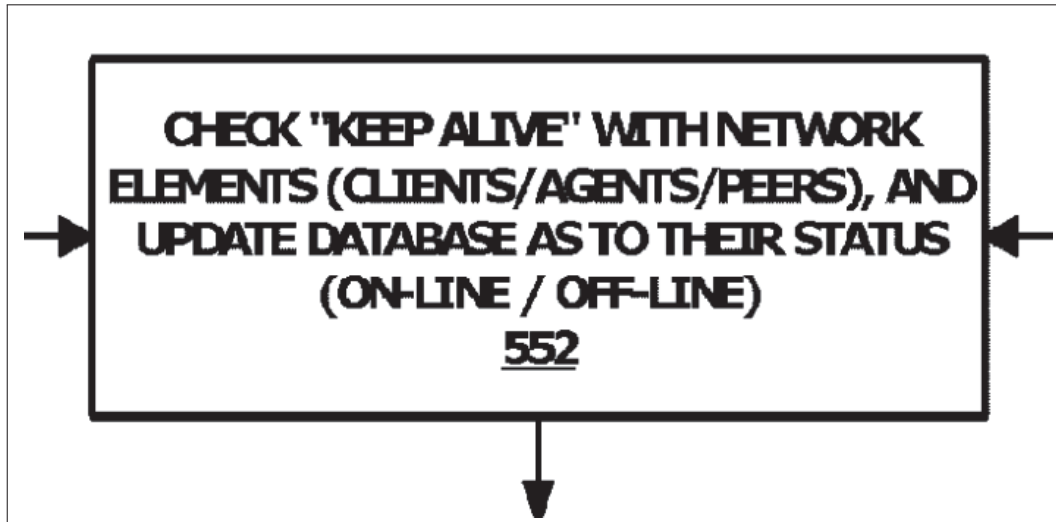
The Shribman '733 publication discloses periodically determining whether agent devices are online. Claim 1 does not specify the device that performs the determining. The Shribman '733 publication discloses two variations.

Ex. 6, Shribman '733 publication discloses:

[0099] ... As shown by block 552, the acceleration server sends "keep alive" signals to the network elements, and keeps track within its database as to which network elements are online.

Ex. 6, Shribman '733 publication, ¶ [0099]. *See also* 166 in Fig. 7 of Ex. 6. Block 552 in Fig. 13 of the publication (which the full figure shows is repeatedly executed in a loop) reflects this as well:

and [0072] (relay of client device IP to first server) *with* '614 patent, Ex. 1 at 107:26-38 (startup) and 108:67-109 (relay of client device IP to first server). It is substantially the same relay mechanism in both cases, and in neither case (*i.e.*, in neither of the prior publication or the '614 patent) is there an embodiment with a transfer by the initiating client device upon its startup, of its IP address directly to the device that operates as the first server. The claims of the '614 patent should not be read in a manner that excludes all of its disclosed embodiments. Furthermore, while Requester understands that reexamination does not directly address written description support under § 112, if the disclosure of the '614 patent in this regard is contended to be sufficient to support this claim limitation, then, by the same measure, the corresponding and equivalent disclosure in the predecessor but prior art Shribman '733 publication should be equally sufficient to anticipate it.



Block 552 in Fig. 13 of the Shribman '733 publication

The referenced "database" makes the disclosed status determination *persistent*, as reflected in items 166 and 312 in Fig. 7:

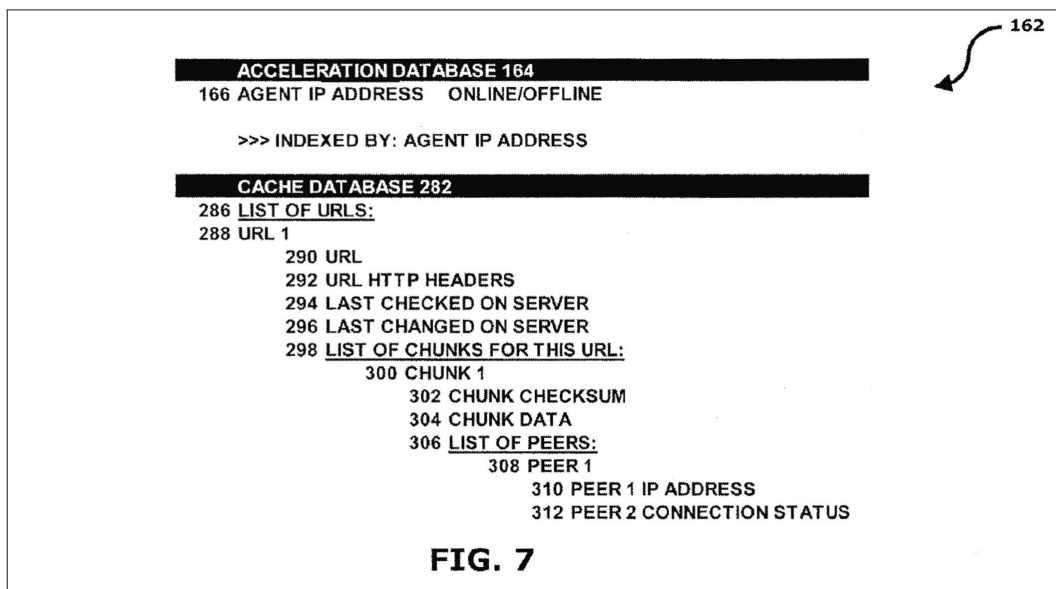


Fig. 7 of the Shribman '733 publication

While item 166 in Fig. 7 reflects a record of the claimed determination in the database of the acceleration server, item 312 reflects a corresponding record in each communication device database as well, indicat-

ing that the communication devices perform corresponding monitoring of each other.

A POSITA understands that “keep-alive” signals are used, as the Shribman ’733 publication explicitly states, to “keep[] track of . . . which network elements are online,” for example, by determining that they are off-line when the keep-alive sender fails to receive a response to its keep-alive signal after a specified timeout period. *See* Ex. 3 ¶ 152.

Thus, certainly under BRI, in the context of the Shribman ’733 publication, the “resource” in question may be viewed as the sum total of the capabilities of the device in its current operating condition to respond to a signal.

Requester submits that it is a reasonable interpretation that a “resource” in the context of claim 1 can mean a combination of device facilities whose aggregate utilization at any given time affects the time it takes for the device to respond to a keep-alive signal.

The “criterion” in this context may be viewed as whether the device responds within a specified time period. The “first state” corresponds to the state of the disclosed database, in reflecting the device as being on-line or off-line as so determined.

This limitation is thus disclosed by the Shribman ’733 publication.

[1.3] responsive to the determining that the utilization of the resource satisfies the criterion, shifting to the first state or staying in the first state;

If the utilization of the resource satisfies the criterion, the method taught in the Shribman ’733 publication teaches to mark the device on-line in the database (or continue such a marking if the database was already in this state), which constitutes shifting to (or staying in) the first state.

This assertion is based on the reasoning that having one of two mutually exclusive entries (on-line or off-line) written in a database represents a “state” of the system, and that changing such entries from one such indication (*e.g.*, on-line) to the other (off-line) constitutes a “shifting” of the state. Requester submits that this is a reasonable interpretation.

The Shribman '733 publication thus discloses shifting to (or staying in) a first state based on whether the utilization of a resource (*i.e.*, the device's collected capacity to respond to a keep-alive message satisfies a timing criterion.

Again, the claim does not say what it is that “shifts” state, and based on the alternatives presented in dependent claims 2 and 3, the generality of claim 1 appears to be intentional. In the case of the Shribman '733 publication, the “state” is manifested in a database entry, which resides on the device doing the monitoring, which can be the acceleration server 162 or any of the communication devices 200 (*see* ¶ [0069], describing each communication device's “list of peers” and “the connection status 312 of the peer.”

[1.4] responsive to the determining that the utilization of the resource does not satisfy the criterion, shifting to the second state or staying in the second state;

Likewise to limitation [1.3], if the utilization of the resource *does not* satisfy the criterion (*i.e.*, a keep-alive signal is sent to the device, but no timely response is received), the method taught in the Shribman '733 publication teaches to mark the device as off-line in the database (or continue such a marking if the database was already in this state), which constitutes shifting to (or staying in) the second state.

Per the disclosure of the Shribman '733 publication, it can be the acceleration server and/or any of the communications devices (which can serve as agents, peers, or clients) that shifts state as claimed, either of which is consistent with the claim language.

The Shribman '733 publication thus discloses this limitation.

[1.5] responsive to being in the first state, receiving, by the client device, a request from the first server

The disclosed method in the Shribman '733 publication sends content retrieval tasks only to those agents marked as online: “choosing one or more client communication device out of all *online* client communication devices” (claim 32 in the Shribman '733 publication). *See also* ¶¶ 38, 66, 69, 80 (The list of agents is created by the acceleration server 162 by finding the communication devices of the communication network 100 that are currently online . . .), and ¶ 99.

Thus, the client device in the Shribman '733 publication receives the content retrieval request (the request) from the requesting client (first server) only responsive to being in the “first state,” *i.e.*, the online state.

In particular, the Shribman '733 publication discloses that the acceleration server 162 sends a list of agents to client 200 (first server) based in part “by finding the communication devices of the communication network 100 that are currently online” (¶ [0080], *i.e.*, responsive to being in the first state, and that as a consequence, the agents (each a “client device”), receives a request from the client (first server):

[0081] As shown by block 360, the client module 224 then sends the original request (*e.g.*, “GET <http://www.aol.com/index.html> HTTP/1.1”) to all the agents in the list received from the acceleration server 162 in order to find out which of the agents in the list is best suited to be the one agent that will assist with this request.

However, as the foregoing reflects is also disclosed, only agents found to be in an on-line state are sent the request. Thus the Shribman '733 publication discloses that, responsive to being in the first state, the client device receives a request from the first server. This occurs at block 360 in Fig. 9.¹⁷

[1.6] performing a task, by the client device, in response to the receiving of the request from the first server

As noted above, the agent/client device receives “the request” from the first server at block 360 of Fig. 9, as described at ¶ [0081]. Responsive thereto, the agent/client device performs a task, which begins at block 382 on Fig. 10, and continuing through the remainder of Fig. 10 and from there through Fig. 11, as described in ¶¶ [0082]-[0089].

Thus, the Shribman '733 publication discloses step [1.6].

¹⁷ Once again, claim 1 does not specify what is “in the first state.” Consistent with the claim language, it can be some other device (*e.g.*, another communication device, or the acceleration server) that is recording the determination of the condition of the client device, and thus “in” the first state, wherein, per the claim preamble, the first client device may only be “associated with” (and not necessarily “in”) the first state as so maintained by that other device. Thus, the acceleration server database, for example, may literally be in the “first state,” meaning that entry 166 in the database (which exists on the acceleration server) is “ONLINE” and the client device itself is *associated with* that state by in fact *being* online (as the acceleration server has determined). The language “responsive to being in the first state [the client device receives something]” only requires the client device to do the receiving. It does not require the client device itself to be the agency that is in the first state. Moreover, since claim 3 contemplates that the first server may do the “determining” based on “receiving . . . the resource utilization from the client device” it makes sense that the state “shift” refers in that case to the state of the record on the determining device. Since there is no basis to read into this claim what agency is in the specified state (where the claim does not so recite), the above-mentioned disclosure of the Shribman '733 publication satisfies the literal language of step [1.5]. See Ex. 3 ¶ 167.

[1.7] wherein the method is further configured for fetching over the Internet a first content identified by a first content identifier from a web server that is distinct from the first server

Per step 1.7, the “task” to be performed by the client device is proxied web content retrieval.

Referring to block 390 and following in Fig. 10, the Shribman ’733 publication discloses two possible responses by an agent to a content request as discussed above in connection with step [1.6]: the first response (blocks 392-396) is if the agent happens to already have information as to how the request may be satisfied locally (from cache), and the second (and alternate) response (blocks 400-406) is if it does not—in which case it fetches the content directly from the origin web server (*i.e.*, “fetching over the Internet a first content identified by a first content identifier from a web server that is distinct from the first server”):

[0089] If the selected agent discovers that it does not have information about this request, or if the selected agent discovers that the information it has is no longer valid, the selected agent needs to load the information directly from the server in order to be able to provide an answer to the requesting client. As shown by block 400, the selected agent then sends the request directly to the server. The selected agent then stores the information it receives from the server (both the headers of the request, as well as chunks of the response itself) in its database, for this particular response to the client, as well as for future use to other clients that may request this data (block 402). The selected agent then prepares a response (list) for the client, where the response includes the protocol headers (if these are the first five chunks), and the checksums of the five chunks, and provides itself as the only peer for these chunks (block 404). This list is then sent back to the client (block 406).

The first content—the information that the agent in this scenario “load[s] directly from the server,” is identified by a first content identifier: The request includes the URL as shown in ¶ [0081] and thus the first content identifier. The “server” mentioned is one that responds to HTTP requests and thus is a web server (see web server 152 in Fig. 3), and is also distinct from the first server.

Thus, the Shribman '733 publication meets this limitation.

[1.8] [and the task comprising:] receiving, by the client device, the first content identifier from the first server;

The first content identifier, as shown in ¶ [0081] of the Shribman '733 publication (referring to block 360 in Fig. 9), is sent by the client device (client 102, first server) to each agent (each a “client device” for purposes of claim 1). Thus, the Shribman '733 publication discloses the client device receiving the first content identifier from the first server, as part of the task that the client device performs responsive to being in the first state.

[1.9] sending, by the client device, the first content identifier to the web server;

Shribman '733 publication, ¶ [0089] (“As shown by block 400, the selected agent then sends the request directly to the server”). Thus, the Shribman '733 publication meets the limitations of step [1.9].

[1.10] receiving, by the client device, the first content from the web server in response to the sending of the first content identifier; and

Shribman '733 publication, ¶ [0089] (“The selected agent [client device] then stores the information it receives from the server (both the headers of the request, as well as chunks of the response itself) [first content] in

its database, for this particular response to the client [first server]"). Thus, the Shribman '733 publication meets the limitations of step [1.10].

[1.11] sending, by the client device, the received first content to the first server.

The Shribman '733 publication discloses in ¶ [0089] that in the scenario being described, the agent (client device) "provides itself as the only peer for these chunks [first content]" and that "[t]his list is then sent back to the client [first server]." Since the agent is the only local source for the requested content, it is all sent from the client device (the agent) to the first server (client 102) when the client requests these chunks from (in this case) the same agent, and the agent send them, per ¶¶ [0090]-[0092]. This disclosure meets the limitations of step [1.11].

* * * * *

In sum, the Shribman '733 publication identically discloses both the "front end" (state shifting, [1.P] and [1.1]-1.6)) and the "back end" (proxy retrieval, [1.7]-[1.11]) steps of claim 1, fully anticipating claim 1.

7.1.2. SNQ Ia (§ 102-Shribman '733 Publication)/Claim 3

3. The method according to claim 1, further comprising periodically or continuously sending, by the client device, the resource utilization to the first server, and wherein the determining is performed by the first server in response to a receiving, by the first server, the resource utilization from the client device.

The Shribman '733 publication teaches tracking the state of the agent device by another device, which sends keep-alive messages to the agent

(periodically or continuously sending), determines if the responses (reflecting resource utilization) are timely (determining), and tracks the results in a database. Ex. 6 ¶ [0099]. Further, as reflected in Ex. 1 ¶ [0069], communication device 200 (which as above maps to the claimed “first server”) maintains a cache database 282, which tracks the connection status 312 of the peers (each corresponding to the claimed “client device”), reflecting wherein the determining is performed by the first server (*i.e.*, by that communication device 200). If the client device (agent or peer) is responding, it then also periodically or continuously sends the responses, indicating an on-line state of resource utilization, to the first server.

The Shribman '733 publication thus meets the limitations of claim 3.

7.1.3. SNQ Ia (§ 102-Shribman '733 Publication)/Claim 4

4. The method according to claim 1, wherein the communication by the client device with the first server is based on, or is according to, TCP/IP protocol or connection.

The base claim, claim 1, taken as a whole, concerns performing a task of retrieving web content. A POSITA would understand that web content typically destined for display in a web browser, as it definitely is in the case of the Shribman '733 publication. See Ex. 6 ¶¶ [0045]-[0046]. As noted as AAPA in the '614 patent, “Web browsers typically use TCP when they connect to servers on the World Wide Web.” Ex. 1 1:61-62. See also Ex. 12 RFC 2616 § 1.4, similarly noting that HTTP content retrieval is typically done over TCP. Indeed HTTP over TCP could not have been avoided, given the large numbers and diversity of client devices contemplated by the disclosure of the Shribman '733 publication. Ex. 3 ¶ 181. The use of TCP

between the client and the server in the context of the process recited in claim 1 is therefore inherent.

Moreover, the Shribman '733 publication teaches a further embodiment in which a communication device/client, mapped as above as the "first server" in claim 1, creates an established TCP connection with an agent (mapped as above as the "first server"). Ex. 6 ¶¶ [0106]-[0107] & Fig. 14. For example, ¶ [0107] states: "To establish a connection, as shown by block 608, the client [first server] issues a TCPIP connect with the primary agent or one of the other agents [each, client devices] if the primary agent does not succeed, to create a connection with the agent."

The Shribman '733 publication thus meets the limitations of claim 4.

7.1.4. SNQ Ia (§ 102-Shribman '733 Publication)/Claim 5

5. The method according to claim 4, further comprising establishing a connection with the first server, and wherein the communication with the first server is over the established connection, and wherein the communicating by the client device with the first server uses TCP, and wherein the connection is established by performing 'Active OPEN' or 'Passive OPEN'.

Claim 5, adds that the TCP connection of claim 4 is an "established connection," which is established *either* by an 'Active OPEN' or a 'Passive OPEN'.

A POSITA knows from Ex. 28 RFC 793 § 2.7 that a TCP connection is by its nature an established connection, and ¶ [0107] quoted above shows this reflected in the disclosure of the Shribman '733 publication itself. A POSITA also knows, again from Ex. 28 RFC 793 § 2.7, that a TCP connection is established by either one or the other of an Active or Passive open,

so the “established connection” and alternative ‘or’ limitations in claim 5 (*i.e.*, “Active OPEN” **or** “Passive OPEN”) do not limit the claim beyond what is already inherent in the TCP protocol.

The Shribman '733 publication thus meets the limitations of claim 5.

7.1.5. SNQ Ia (§ 102-Shribman '733 Publication)/Claim 7

7. The method according to claim 1, wherein the steps are sequentially executed.

The Shribman '733 publication discloses the same sequence of steps in the same order as set forth in claim 1.

It is true that in the Shribman '733 publication step [1.8] (client receives the first content identifier from the first server) occurs as part of step [1.6], because “the request” that the client device receives from the first server (per step [1.6]) already includes the first content identifier, and it is not resent.

That said, in accordance with BRI, claim 1 can be read to define two processes, the first concerning the steps of determining the client device's state of availability to handle a task, and the second concerning the steps in performing the task (of proxied content retrieval) itself. The steps of each of these processes are performed in the sequence written, in the disclosure of the Shribman '733 publication. The fact that these processes are overlapping does not negate the limitations of claim 7.

The above interpretation of claim 1 further makes sense in that it would be redundant and inefficient, and provide no benefit, to first make a request to perform a content retrieval task, only to have to follow up later with a separate request specifying the actual content to be retrieved.

The Shribman '733 publication thus meets the limitations of claim 7, as so reasonably interpreted.

7.1.6. SNQ Ia (§ 102-Shribman '733 Publication)/Claim 8

8. The method according to claim 1, wherein the first identifier comprises an IP address that is in IPv4 or IPv6 form.

The Shribman '733 publication discloses that the first identifier (*i.e.* of the agent) is an IP address. ¶¶ [0069], [0072] and Fig. 7, showing each peer device having an IP address 310. IPv4 or IPv6 forms are the only two possibilities. *See* Ex. 3 ¶ 192.

The Shribman '733 publication thus meets the limitations of claim 8.

7.1.7. SNQ Ia (§ 102-Shribman '733 Publication)/Claim 9

9. The method according to claim 1, wherein the client device is further storing, operating, or using, a client operating system.

The Shribman '733 publication, Ex. 6 ¶ [0045], discloses that each client device further stores, operates, and uses, a client operating system.

The Shribman '733 publication thus meets the limitations of claim 9.

7.1.8. SNQ Ia (§ 102-Shribman '733 Publication)/Claim 13

13. The method according to claim 1, further comprising executing an application, and wherein the application comprises a web browser.

The Shribman '733 publication teaches that the client device may run a web browser. Ex. 6 ¶¶ [0045], [0046], [0057], [0058], [0078], and [0095].

The Shribman '733 publication thus meets the limitations of claim 13.

7.1.9. SNQ Ia (§ 102-Shribman '733 Publication)/Claim 17

17. The method according to claim 1, for use with a set threshold value, and wherein the criterion is satisfied when the resource utilization is above or below the threshold.

As discussed, a timeout value is inherently used with a keep-alive signal as disclosed in the Shribman '733 publication. The timeout value acts as a threshold value as in this claim.

The Shribman '733 publication thus meets the limitations of claim 17.

7.1.10. SNQ Ia (§ 102-Shribman '733 Publication)/Claim 25

25. The method according to claim 1, further comprising periodically sending, by the client device, a message that comprises a status of the client device, or is in response to the status of the client device.

As noted above, the Shribman '733 publication discloses servers that send periodic keep-alive messages to the client device, as well as server and peer databases that record the client's responses to those messages. It follows that these disclosures also necessarily reflect that the client device in the disclosure is periodically responding to the first server (*e.g.* a peer) with messages in response to the status of the client device, *i.e.*, that the client device is available. This is so because the database entries 166 and 312 in Fig. 7 of the Shribman 733 publication can only be explained as resulting from such messages returned by the client device in response to the keep-alive messages.

The Shribman '733 publication thus discloses the limitations added by claim 25.

7.1.11. SNQ Ia (§ 102-Shribman '733 Publication)/Claim 26

26. The method according to claim 25, wherein the status is associated with being in the first or second state, and wherein the message is sent over the Internet to the first server.

The Shribman '733 publication, Ex. 6, ¶ [0099] discloses a peer status that is associated with being (or not being) in the online state and a message (when it is in the first state) reflecting that status is sent over the Internet to client 102 (first server).

The Shribman '733 publication thus discloses the limitations added by claim 26.

7.1.12. SNQ Ia (§ 102-Shribman '733 Publication)/Claim 29

29. The method according to claim 1, wherein the web server uses HyperText Transfer Protocol (HTTP) and responds to HTTP requests via the Internet, and wherein the sending of the first content identifier to the web server comprises a HTTP request, or wherein the communication with the web server is based on, or uses, HTTP persistent connection, and wherein the first content includes, consists of, or comprises, a part or whole of files, text, numbers, audio, voice, multimedia, video, images, music, or computer program, or wherein the first content includes, consists of, or comprises, a part of, or a whole of, a web-site page.

The Shribman '733 publication discloses this limitation. As reflected in Ex. 6, ¶ [0081], the web server uses HTTP protocol and responds to HTTP requests via the Internet. Per ¶ 0089, the client device (agent)

sends a content request (referred to as “the request”) “directly to the [web] server.” The antecedent of “the request” in ¶ [0089] is the HTTP request disclosed in Par. [0081] (the example given is the HTTP request “GET http://www.aol.com/index.html HTTP/1.1”). The fact that a “web” server is involved is made clear in ¶ [0080], referring to “Web server 152.”

The foregoing addresses the limitations of claim 29 up to the “or” conjunction therein. Such disclosure of one of the alternatives in a claim such as claim 29 that is phrased in the alternative is sufficient in itself to anticipate the claim. See MPEP 2131.02.

7.2. SNQ Ib: Obviousness of Claims 1-5, 7-9, 13, 17, 25-26, and 29 over the Shribman '733 publication in view of Liu

7.2.1. SNQ Ib (§ 103-Shribman '733 Publication + Liu)/ Claim 1

Requester has argued above that the Shribman '733 publication anticipates claim 1, on the basis that the Shribman '733 publication's disclosure, wherein a device separate from the claimed client device determines and maintains the first/second state based on communications with the client device, and wherein this state is maintained on the other device is “associated with” the actual condition of the client device, is sufficient under BRI to meet the literal claim language, which does not expressly identify the device that is required to be “in” the referenced state.

Should the Examiner believe that, notwithstanding BRI, claim 1 further requires the recited states to be actual states *of the client device*, and that it must be the client device itself that must “shift” its own state as

otherwise recited, then Requester submits in the alternative that claim 1 is obvious over the Shribman '733 publication in light of Liu, Ex. 29.

As will be addressed below, Liu discloses device monitoring and selection steps meeting even a more narrow construction of the claims, and would be an obvious combination with the Shribman '733 publication, given the latter's own suggestions as to monitoring the status of the retrieval devices.

To begin with, there was a considerable volume of background prior art directed content retrieval through intermediary devices. The background references teach both the general use of proxies for intermediated content retrieval over the Internet, as well as techniques for deploying groups of proxies, and choosing a proxy from the group in order to perform a specific retrieval. *See, e.g.*, Ex. 13 at 152 ("Talking to Other Squids"), 176 (concerning "CARP" (Cache Array Routing Protocol) and having a "user agent" (client) choose a particular "cache" (proxy) from an "array" of such caches); Ex. 14 at 116 (describing the "ICP" (Internet Cache Protocol) to discover which proxy from a plurality of proxies to use for a retrieval, including, for example, "determining the relative speed of each proxy server that is queried").

Thus, the general problem addressed by claim 1 of the '614 patent, that of selecting an appropriate proxy from a group of provided proxy devices—and even a solution (*e.g.*, as in Luotonen) based on the performance capability of the proxies—had already been addressed in general background references.

The Shribman '733 publication further provides another specific example of the same, including specifically tracking the state of the various

deployed proxy devices to determine whether to use them for content retrieval. See discussion at page 80 above.

Liu, cited herein, further addresses the specific solution provided by the '614 patent, wherein it is necessary to filter provided helper devices based on their state of availability. Like the '614 patent, Liu teaches to do this filtering by having the helper device itself monitor the “state” of its own availability, to be able to verify that the device is appropriate to continue to use for the specified task. Thus, a POSITA, who already knew (*e.g.*, from the Shribman '733 publication, as well as from general texts such as Squid and Luotonen) to make use of a plurality of proxies to assist in performing content retrieval tasks, and who already knew (*e.g.*, from these same references) to choose among the provided proxies based on their suitability for the desired task, would have found it obvious to look to Liu, which taught, in an analogous network deployment, to make such a selection simply by adapting the helper device as was done in Liu, to determine and report *its own* state of availability for the specified task, to facilitate the selection of a suitable helper by other devices. The fact that the helper device in the context of the '733 patent happens to be a distributed content retrieval proxy, as opposed to a distributed information layer agent (as in Liu), makes no difference operationally, and in either case the implementation of a state machine as in Liu would be routine and with a high expectation of success. Ex. 3 ¶ 212.

The foregoing becomes further apparent when considering the details of Liu. Liu discloses a distributed system for detecting and responding to distributed denial of service (DDoS) attacks. See, *e.g.*, Ex. 29 at Abstract. The system of Liu deploys a plurality of agents to detect DDoS attacks.

Each agent runs its own finite state machine, operating per a state transition diagram as follows:

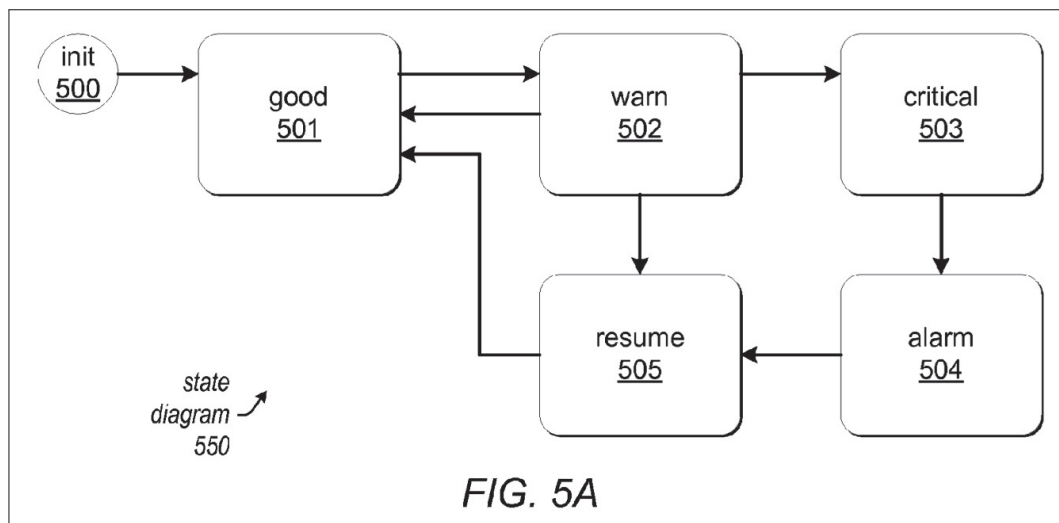


Fig. 5A from Liu, showing agent's FSM

Requester points out the similarity of the above diagram to Fig. 30 of the '614 patent, which the '614 patent also describes as a "state diagram":

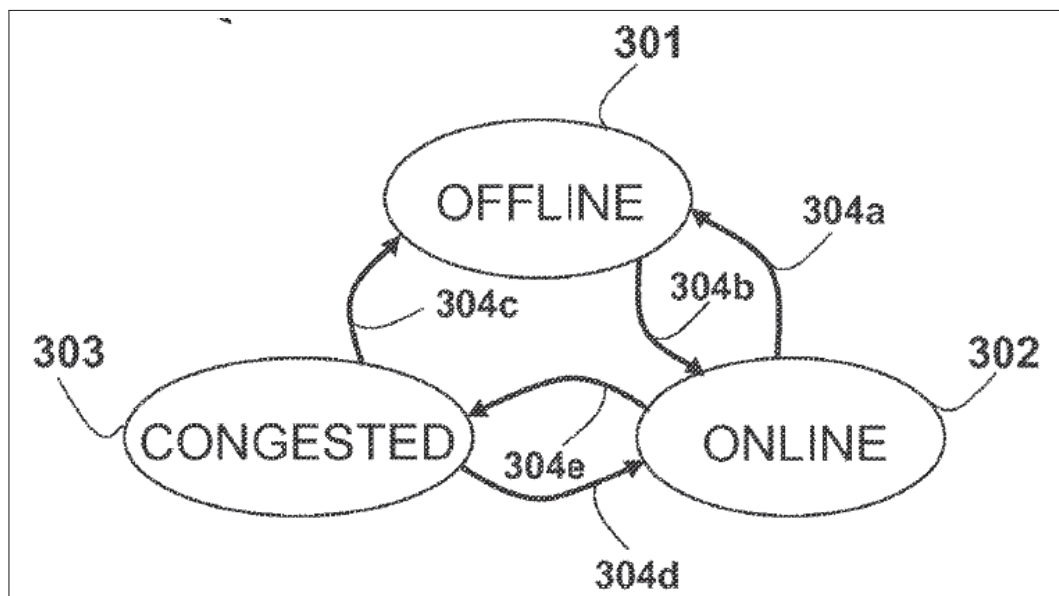


Fig. 30 from the '614 patent (cropped)

In Liu, if the agent goes into an undesirable state, one of the responses of the system is to remove the agent from the deployed “pool” of agents. *See id.* ¶ [0063]. State transitions are driven by events such as comparing an operating metric (resource) to a threshold. *See id.* ¶ [0058].

Liu reflects an alternate approach to maintaining state based on resource utilization, where (as in the particular embodiment depicted in Fig. 30 of the ’614 patent) the state is both determined and maintained *on the client device*.

As addressed in Section 6.3 above, with regard to anticipation under § 102, Requester takes the position that, under BRI, claim 1 of the ’614 patent is not limited to where the state of the client device is tracked *on the client device itself*. Ex. 3 ¶ 217.

Nevertheless, should the Examiner decide on a narrower interpretation, wherein the claimed shifting of states must be performed by the client device, on the client device, Requester submits that this narrower formulation would have been obvious in any case, over the Shribman ’733 publication in view of Liu. This is so, given the disclosures of tracking client device state in the Shribman ’733 publication, and the further disclosure in Liu of *a client device itself* doing such tracking, under circumstances and for reasons similar to those set forth in the Shribman ’733 publication.

In this regard, it would have been obvious to apply the technique of using a client-side state machine, as in Liu, to implement the condition of making sure that the client device is online and therefore available, as taught in the Shribman ’733 publication.

Using a state machine for such purposes is taught by Liu, as described above. While Liu is sufficient to document this further teaching, it is also

noted that Liu of course did not *invent* the use of state machines for such purposes. The technique of using finite state machines on a device, to change how the device represents itself to other objects in a system, was also widely-known background prior art to any POSITA in 2013. See, for example, the well known “Gang of Four” (GOF) book on Design Patterns (1994) (Ex. 27), disclosing a “State” design pattern, based on an underlying state machine implemented within a device. In the words of the Gang of Four, the State pattern does the following:

Allow an object to alter its behavior when its internal state changes.

The object will appear to change its class.

Ex. 27 at 305. Using a state machine, as taught by Liu, is obvious, further in view of background knowledge, such as design principles taught in GOF, where it is desired that an object (such as a client device in a network deployment) will change its behavior when its internal state changes.¹⁸

There is considerable motivation to combine client device state tracking as taught in the Shribman ’733 publication, with a process for maintaining and shifting state on the client device itself, as taught by Liu in an analogous setting (in which client devices were likewise deployed to perform network functions), to thus arrive at the claimed invention of claim 1. Performing the state determination and using the results to drive a FSM, directly on the client device, requires less communication among devices and promotes a more reliable determination, as a POSITA would recognize that the requisite data for these determinations originates locally to the device, and performing the determination on the device itself need not wait for handshaking with other devices. Ex. 3 ¶ 222. Moreover, the Shribman

¹⁸ The ’614 patent also specifically references the use of “object-oriented environments” (addressed in the GOF reference) for programming the disclosed devices. Ex. 1, 171:18-30.

'733 publication already suggests maintaining a record designed to reflect the state of the client device, for the same reason, to verify that the client devices are actually available to perform their desired functions. Given these suggestions and motivations in the references themselves, and the fact that Liu is highly analogous, the combination of the Shribman '733 publication and the locating of state determination and maintenance to the client device (as in Liu) would have been obvious. Moving this functionality to the client device was a routine type of reallocation of functionality between connected devices in a system (see Ex. 3 ¶ 223), and would have been an obvious design choice, also providing the further advantage of encapsulating functionality on the client device (among other things, thereby checking state internally and avoiding the need for responding to frequent polling by other devices when there is no state change), with predictable results. In all other respects, this combination meets all the limitations of claim 1, for the reasons already given. See Ex. 3 ¶ 223.

As noted with regard to § 102 above, Requester also believes that the Shribman '733 publication sufficiently discloses step [1.1] under BRI to be anticipating in itself. To the extent the Examiner requires further support for the limitation of communicating the client device's IP address on its startup, specifically to the first server (to which the acceleration server of the Shribman '733 publication *relays* the IP address), Requester submits that passing on the IP address of the registering device in this manner, *directly* to the device serving as the first server, would have been an obvious variation on what the Shribman '733 publication was already disclosing. Functionally, claim step [1.1] provides for the client device to register itself on startup, with the proxy assignment mechanism, for later use as a content retrieval proxy, so that the system knows about the devices at its

disposal. The Shribman '733 publication clearly discloses that same type of startup functionality (Ex. 6 ¶¶ [0066] as well as [0072], wherein the client device on its own startup signs in with the acceleration server). It also discloses a database in each client device (of which the first server is one), of other client device IP addresses (see item 310 in Fig. 7), including the client devices that can serve as proxies. It discloses updating client devices as to agent assignments (to handle retrieval from particular ranges of origin servers) when new client devices join (see ¶ [0066] (last sentence)). To the extent the disclosure in ¶ [0066] does not expressly spell out automatically populating the database item 310 data with corresponding IP addresses of other clients *when they join*, it would have been an obvious design choice to have the acceleration server simply relay each newly registered IP address to existing registered client devices *immediately* as each new device signed in, and for the receiving devices to record the IP addresses in their respective local databases, rather than waiting for an actual content request in order to fill in this information. Ex. 3 ¶ 224.

7.2.2. SNQ Ib (§ 103-Shribman '733 Publication + Liu)/ Claim 2

2. The method according to claim 1, wherein the determining is performed by the client device.

Claim 2 addresses the exact situation that arises with the combination of the Shribman '733 publication and Liu. Under this combination, the determination of claim 1 is performed by the client device.

Thus, the combination represented by claim 2 would have been obvious. Ex. 3 ¶ 226.

7.2.3. SNQ Ib (§ 103-Shribman '733 Publication + Liu)/ Claims 3-5, 7-9, 13, 17, 25-26, and 29

As to claims 3-5, 7-9, 13, 17, 25-26, and 29, Requester has separately argued above that the Shribman '733 publication anticipates claims 3-5, 7-9, 13, 17, 25-26, and 29 by disclosing the limitations of claim 1 and the separate limitations of each of claims 3-5, 7-9, 13, 17, 25-26, and 29. To the extent if any that the Shribman '733 publication is not deemed to fully anticipate claim 1, then Liu cures any such deficiency as discussed above, and the same rationale as expressed above that would have made it obvious to have combined Liu with the Shribman '733 publication as to claim 1 would also apply with respect to each of claims 3-5, 7-9, 13, 17, 25-26, and 29, because the Shribman '733 publication itself likewise discloses the further limitations of each of those claims.

7.3. SNQ Ic: Obviousness of Claims 2-6, 8-10, 14-27, and 29 over the Shribman '733 publication in view of Sig- urdsson and/or Chauhan

7.3.1. SNQ Ic (§ 103-Shribman '733 Publication + Sigurds- son and/or Chauhan)/Claim 2

2. The method according to claim 1, wherein the determining is per- formed by the client device.

As noted by the Examiner during original prosecution (Ex. 2 at 294), Sigurdsson teaches wherein the determining is performed by the client device. Ex. 7 ¶ [0061], lines 7-8, “monitoring polling by the client.”

Thus, the combination represented by claim 2 would have been obvious. Ex. 3 ¶ 229.

7.3.2. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson and/or Chauhan)/Claim 3

3. The method according to claim 1, further comprising periodically or continuously sending, by the client device, the resource utilization to the first server, and wherein the determining is performed by the first server in response to a receiving, by the first server, the resource utilization from the client device.

As noted above with regard to claim 2, the Shribman '733 publication already provides for monitoring by the first server of the availability of the client device, categorizing the client device as “online” or “offline.” In the referenced disclosure (Ex. 6 ¶ [0099]), the device serving as the first server makes this determination periodically, by tracking the results of keep-alive signals in a database on the first server, as reflected in database entry 312 in Fig. 7. The client device also periodically or continuously sends responses to the keep-alive messages, to the first server, as indicated by a POSITA’s knowledge that this is how keep-alive messaging works, and the fact that the disclosure shows the first server (communication device 200) maintaining a database record of the determined state of the client device. To the extent these steps are not deemed sufficiently explicit or inherent in the Shribman '733 publication’s disclosure, they certainly would have represented an obvious implementation to arrive at database entry 312 as expressly disclosed therein. Ex. 3 ¶ 230.

Moreover, as noted by the Examiner during original prosecution (Ex. 2 at 294), Sigurdsson provides a similar approach: “Sigurdsson teaches periodically or continuously sending, by the client device, the resource utilization to the server (sec [0006], lines 8-10, which discloses a client transmitting content-related metadata to the server, and wherein the de-

termining is performed by the server in response to a receiving, by the server, the resource utilization from the client device (sec [0007], lines 1-8, which discloses determining that a server is configured to transmit content to a client in response to receiving metadata from a client).” A POSITA would have been motivated to make the obvious and simple modification to incorporate the further features of Sigurdsson, of periodically sending performance metadata to the server so that the server could determine client device availability based thereon, into the framework of the Shribman ’733 publication to obtain a more versatile tracking of the client device’s state and availability. See Ex. 3 ¶ 231.

A POSITA knowing the foregoing would have found claim 3 obvious. Ex. 3 ¶ 232.

7.3.3. SNQ Ic (§ 103-Shribman ’733 Publication + Sigurdsson and/or Chauhan)/Claims 4 and 5

4. The method according to claim 1, wherein the communication by the client device with the first server is based on, or is according to, TCP/IP protocol or connection.

5. The method according to claim 4, further comprising establishing a connection with the first server, and wherein the communication with the first server is over the established connection, and wherein the communicating by the client device with the first server uses TCP, and wherein the connection is established by performing ‘Active OPEN’ or ‘Passive OPEN’.

In addition to being implicit in the Shribman ’733 publication as noted above, the use of TCP between client and server is also obvious in view of references such as Chauhan. As noted by the Examiner during original

prosecution, “Chauhan et al. teaches wherein the communication by the client device with the server is based on, or is according to, TCP/IP protocol or connection (sec [0286]).” Ex. 2 at 294. TCP is also a generally applicable Internet standard protocol, further supplying a motivation to combine. As also discussed above, ActiveOPEN and PassiveOPEN are the only two choices for opening a connection under the TCP standards, and it therefore would likewise have been obvious—indeed, mandatory) to use one of the two available methods.

7.3.4. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdson, and/or Chauhan)/Claim 6

6. The method according to claim 5, wherein the communication by the client device with the first server is based on, or is according to, a Virtual Private Network (VPN) and the established connection is using a tunneling protocol.

As noted in Ex. 2 at 295, during original prosecution the Examiner found this limitation obvious in view of Chauhan: “Regarding claim 6, Chauhan et al teaches wherein the communication by the client device with the server is based on, or is according to, a Virtual Private Network (VPN) (sec [0050], lines 8-9) and the established connection is using a tunneling protocol (sec [0107], lines 11-12).”

It would have been obvious to a POSITA to combine the Shribman '733 publication with Chauhan because incorporating the secure data transmission provisioning mechanism of Chauhan within the content transmission system of the Shribman '733 publication would provide the predictive result of allowing for more effective network security and secure transmission of data between peer clients and a network server when implementing

an encrypted channel for an increased level of security via transmission through implemented network tunnels. Ex. 3 ¶ 235.

7.3.5. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdson, and/or Chauhan)/Claim 8

The method according to claim 1, wherein the first identifier comprises an IP address that is in IPv4 or IPv6 form.

As noted above in connection with the Shribman '733 publication, IPv4 and IPv6 are the only two possibilities for the Internet Protocol under existing standards. See 7.1.6.

In addition, as noted in the prosecution history, “Chauhan et al teaches wherein the first identifier comprises an IP address that is in IPv4 or IPv6 form (sec [0207], lines 7-8).” See Ex. 2 at 295. It would have been obvious to have chosen one of the other of IPv4 and IPv6 as disclosed in Chauhan, since Chauhan addresses similar problems of Internet communication and IPv4 and IPv6 are the only two possibilities under the applicable Internet standards.

7.3.6. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdson, and/or Chauhan)/Claim 9

9. The method according to claim 1, wherein the client device is further storing, operating, or using, a client operating system.

As discussed above, the Shribman '733 publication discloses that each client device further stores, operates, and uses, a client operating system. See Ex. 6 ¶ [0045].

In addition, as noted in the prosecution history, “Chauhan et al teaches wherein the client device is further storing, operating, or using, a client

operating system (sec [0089], lines 14-16).” Ex. 2 at 295. Chauhan addresses similar problems as those addressed in the ’614 patent, also using client computing devices, which would obviously be provisioned with an operating system, as disclosed in both the Shribman ’733 publication and Chauhan.

7.3.7. SNQ Ic (§ 103-Shribman ’733 Publication + Sigurdson, and/or Chauhan)/Claim 10

10. The method according to claim 9, wherein the client operating system consists or, comprises of, or is based on, one out of Microsoft Windows 7, Microsoft Windows XP, Microsoft Windows 8, Microsoft Windows 8.1, Linux, and Google Chrome OS.

As noted in the prosecution history, “Regarding claim 10, Chauhan et al teaches wherein the client operating system consists or comprises of or is based on, one of Microsoft Windows 7, Microsoft Windows XP (sec [0089], lines 14-16). Microsoft Windows 8, Microsoft Windows 8.1, Linux, and Google Chrome OS.” Ex. 2 at 295.

A POSITA could readily have used any of these operating systems in conjunction with the disclosures of the Shribman ’733 publication, with predictable results. These are all widely deployed and well-known operating systems and, given the ’614 patent’s contemplation that general purpose devices could serve as clients, it would have been obvious to a POSITA to have selected one of these common operating systems for the client device. See Ex. 1 at 83:4-15.

7.3.8. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson, and/or Chauhan)/Claim 14

14. The method according to claim 13, wherein the web browser is a mobile web browser.

As noted, the Shribman '733 publication discloses that the client runs a web browser as an application, and also teaches (as claimed in claim 11) that the client may run a mobile operating system.

As noted in the prosecution history, Sigurdsson et al teaches wherein the web browser is a mobile web browser (Fig. 4, '104 & '406). *See* Ex. 2 at 295. A mobile web browser would have been an obvious choice where the client needed to run a web browser on a mobile OS. Ex. 3 ¶ 243.

7.3.9. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson and/or Chauhan)/Claim 15

15. The method according to claim 1, wherein the client device comprises, or consists of, a portable or mobile device.

As noted in the prosecution history, “Sigurdsson et al teaches wherein the client device comprises, or consists of, a portable or mobile device (fig. 4).” *See* Ex. 2 at 295. It would have been obvious to do likewise, given that the Shribman '733 publication expressly discloses running a mobile OS.

7.3.10. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson and/or Chauhan)/Claim 16

16. The method according to claim 15, wherein the mobile device comprises a smartphone.

As noted in the prosecution history, “Sigurdsson et al teaches wherein the mobile device comprises a smartphone (fig. 4).” Ex. 2 at 296. This

also would have been obvious in view of the fact that most mobile devices as of the 2014 claimed priority date were smartphones.

7.3.11. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson and/or Chauhan)/Claim 17

17. The method according to claim 1, for use with a set threshold value, and wherein the criterion is satisfied when the resource utilization is above or below the threshold.

As noted in the prosecution history, “Sigurdsson et al teaches for use with a set threshold value, and wherein the criterion is satisfied when the resource utilization is above or below the threshold (sec [0008], lines 6-11 & [0012], which disclose transmitting data between clients only in the event that a peer client doesn’t have a bandwidth that exceeds a pre-determined threshold).” Ex. 2 at 296. Adding this feature would have been obvious, given that a timeout threshold value for responses from the client was already implicit in the server’s use of keep-alive messages, as disclosed in the Shribman ’733 publication.

7.3.12. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson and/or Chauhan)/Claim 18

18. The method according to claim 1, wherein the resource comprises, or consists of, a hardware component in the client device.

As noted in the prosecution history, “Sigurdsson et al teaches wherein the resource comprises, or consists of, a hardware component in the client device (fig./ 1 & sec [0060], Lines 1-3, which disclose determining available bandwidth on each client ’102 & ’104).” Ex. 2 at 296.

While the Shribman '733 publication teaches a resource comprising the collected facilities of a device to response to a message, it would have been obvious to use discrete resources, such as available bandwidth, as disclosed in Sigurdsson, for the same purpose.

7.3.13. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson and/or Chauhan)/Claim 19

19. The method according to claim 18, wherein the hardware component comprises, or consists of, a processor or Central Processing Unit (CPU) operation in the client device.

As noted in the prosecution history, “Sigurdsson et al teaches wherein the hardware component comprises, or consists of, a processor or Central Processing Unit (CPU) operation in the client device (fig. 9).” Ex. 2 at 296; *see also* Ex. 7 at ¶¶ [0008], [0105]; Ex. 8 ¶ [0296]; Ex. 16 ¶ [0025], [0050].

As in claim 18, the use of any single hardware resource whose usage would affect the ability to respond to a message or perform a task, as in the case of the use of CPU utilization for this purpose in Sigurdsson, would have been an obvious modification to the Shribman '733 publication.

7.3.14. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson and/or Chauhan)/Claim 20

20. The method according to claim 19, wherein the resource utilization is based on, or comprises, the processor or CPU time of executing one or more threads or processes, wherein the resource utilization is based on, or comprises, the processor or CPU idling time, or wherein the resource utilization is based on, or comprises, the processor or CPU executing a system idle process.

As noted in the prosecution history, “Chauhan et al teaches wherein the resource utilization is based on, or comprises, the processor or CPU time of executing one or more threads or processes, wherein the resource utilization is based on, or comprises, the processor or CPU idling time (sec [0155], lines 8-10, ‘terminating an execution of a virtual machine’), or wherein the resource utilization is based on, or comprises, the processor or CPU executing a system idle process.” Ex. 2 at 296; *see also* Ex. 16 ¶¶ [0025], [0050].

Claim 20 thus reflects the implementation of claim 19, which could obviously be accomplished by using the same mechanisms as taught in Chauhan, with predictable results.

7.3.15. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson and/or Chauhan)/Claim 21

21. The method according to claim 18, wherein the hardware component comprises, or consists of, a memory in the client device, and wherein the resource utilization is based on, or comprises, an amount of used or unused location or space of the memory.

As noted in Ex. 2 at 296: “Sigurdsson et al teaches wherein the hardware component comprises, or consists of, a memory in the client device (sec [0105], lines 1-2), and wherein the resource utilization is based on, or comprises, an amount of used or unused location or space of the memory (sec [0008], lines 7-12).”

For the reasons set forth above regarding claim 19 (CPU utilization), it would have been equally obvious to use memory utilization, as also taught in Sigurdsson, as indicative of the client device’s ability to respond to a message or perform a task.

7.3.16. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson and/or Chauhan)/Claim 22

22. The method according to claim 1, wherein the resource comprises, or consists of, input or output capability.

As noted in Ex. 2 at 297: “Sigurdsson et al teaches wherein the resource comprises, or consists of input or output capability (sec [0051], lines 10-11, which discloses available resource capacities at each client device).”

This is very similar to what the Shribman '733 publication by itself already teaches, and an obvious variation (if not already implicit).

7.3.17. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson and/or Chauhan)/ Claim 23

23. The method according to claim 22, wherein the resource comprises, or consists of, communication bandwidth of communication with another device over the Internet.

As noted in Ex. 2 at 297: Sigurdsson et al teaches wherein the resource comprises, or consists of communication bandwidth of communication with another device over the Internet (sec [0051], Line 11).

As with, *e.g.* claims 18 and 22, keeping track of communication bandwidth, as disclosed in Sigurdsson, goes to the same considerations of the ability of the client to respond to a message or perform a task, and would have been an obvious adaptation of what is already disclosed by the Shribman '733 publication.

7.3.18. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson and/or Chauhan)/Claim 24

24. The method according to claim 23, wherein the resource comprises, or consists of, communication bandwidth of communication with the first server over the Internet, or wherein the resource utilization is based on, or according to, IETF RFC 2914.

As noted in Ex. 2 at 297: “Sigurdsson et al teaches ‘wherein the resource comprises, or consists of, communication bandwidth of communication with the server over the Internet (sec [0079], lines 7-10), or wherein the resource utilization is based on, or according to IETF RFC 2914.”

As with claim 23, concerning monitoring a resource that is communication bandwidth with “another device,” it is a small and obvious step to focus on the situation where the other device is the “first server” (as taught in Sigurdsson), especially where, as here, (per claim 1) it is the first server that is parcelling out the content retrieval tasks.

7.3.19. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson and/or Chauhan)/Claim 25

25. The method according to claim 1, further comprising periodically sending, by the client device, a message that comprises a status of the client device, or is in response to the status of the client device.

In addition to the disclosures in this regard in the Shribman '733 publication itself (Ex. 6, ¶ [0099]), as noted by the Examiner in prior examination, Ex. 2 at 297: “Sigurdsson et al teaches periodically sending, by the client device, a message that comprises a status of the client device, or is in response to the status of the client device (sec [0061], lines 6-8,

which discloses determining online or offline status of each client, by each client).” The original Examiner further explained:

The examiner maintains that par [0061], lines 6-8 of Sigurdsson, which discloses determining online or offline status of each client, by each client is obvious in light of sending, by the client device, a message that comprises a status of the client device because (contrary to the applicant’s argument that the status is claimed status must solely be drawn to the entity that the examiner mapped to the status in claim 1) a status can be drawn to a plurality of client devices status as claim 25 doesn’t require the periodically collected status to be correlated to the same status information in claim 1.

Ex. 2 at 289.

Thus, the extent, if any, that claim 25 is not deemed anticipated by the Shribman ’733 publication, as set forth above, it would have been obvious, in order for the acceleration server and client devices of that publication (including the client device that acts as the first server), to follow the implementation of Sigurdsson, generating its database entries as to the status of client devices (*e.g.*, entry 312 in Fig. 7 of the Shribman ’733 publication), by receiving and recording responses to the disclosed keep-alive messages, which would have been sent periodically in response to the periodically sent keep-alive messages to each client device, when the client device was online, thus satisfying the limitations of claim 25.¹⁹ In view of Sigurdsson, the foregoing would have been a very obvious way to implement the on-line-off-line client device state tracking already disclosed by the Shribman ’733 publication.

¹⁹ If the client device was off-line, no response would be received within a set timeout period and, because this is how keep-alive messages were conventionally used the absence of a response during the timeout period would result in the database being marked to reflect that the client device was off-line. Ex. 3 ¶ 263.

7.3.20. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson and/or Chauhan)/Claim 26

26. The method according to claim 25, wherein the status is associated with being in the first or second state, and wherein the message is sent over the Internet to the first server.

The obviousness showing above with regard to claim 25 applies to claim 26 as well. Claim 26 additionally specifies only that the status conveyed by the message from the client device is associated with being in the first or second state, and that the message is sent over the Internet to the first server.

The disclosures relied upon above with regard to claim 25 already cover these additional limitations. When the client responds to the keep-alive message it sends a message associated with being in the first (online) state. The message is sent over the Internet, as the client devices of the Shribman '733 publication are deployed in the Internet. *See, e.g.,* Ex. 6 ¶¶ [0002], [0058]. The message is received by the first server, because the first server is also a client device, and every client device according to the Shribman '733 publication disclosure has a database 282 which notes the connection status 312 of other client devices with which it deals, which results from such messages (or which it would be obvious to implement in this manner in view of the disclosures of Sigurdsson cited in connection with claim 25).

7.3.21. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson and/or Chauhan)/Claim 27

27. The method according to claim 25, wherein the message comprises, or is based on, an 'heartbeat' message, and wherein the time period between multiple messages sent is at least 10 milliseconds, 20

milliseconds, 30 milliseconds, 50 milliseconds, 100 milliseconds, 1 second, 2 seconds, 3 seconds, 5 seconds, 10 seconds, 20 seconds, 30 seconds, 50 seconds, or 100 seconds, 1 minute, 2 minutes, 3 minutes, minutes 5, or 10 minutes.

As noted in Ex. 2 at 297-298 (prior examination), Sigurdsson teaches wherein the message comprises, or is based on, an “heartbeat” message (¶ [0061], lines 11-13), and wherein the time period between multiple messages sent is at least 10 milliseconds, 20 milliseconds, 30 milliseconds, 50 seconds, 30 seconds, 50 seconds, or 100 seconds, 1 minute, 2 minutes (¶ [0045], lines 14-15), which discloses implementing set intervals for posting of client content of 3 minutes, 5 minutes, or 10 minutes. Setting a specified time period between multiple keep-alive messages, to the extent not inherent in the Shribman '733 publication, would have been an obvious implementation to incorporate into the techniques taught by the Shribman '733 publication in view of the cited disclosures of Sigurdsson. The frequency of such messages, including the specific frequencies listed in claim 27, would have been a routine design choice and obvious. Ex. 3 ¶ 267.

7.3.22. SNQ Ic (§ 103-Shribman '733 Publication + Sigurdsson and/or Chauhan)/Claim 29

29. The method according to claim 1, wherein the web server uses HyperText Transfer Protocol (HTTP) and responds to HTTP requests via the Internet, and wherein the sending of the first content identifier to the web server comprises a HTTP request, or wherein the communication with the web server is based on, or uses, HTTP persistent connection, and wherein the first content includes, consists

of, or comprises, a part or whole of files, text, numbers, audio, voice, multimedia, video, images, music, or computer program, or wherein the first content includes, consists of, or comprises, a part of, or a whole of, a web-site page.

As discussed above, claim 29 is written in the alternative, and the Shribman '733 publication is anticipating because it discloses the first alternative.

However, the second alternative is also obvious. The Shribman '733 publication itself discloses content of the types recited in the claim, *e.g.*, chunks that comprise the contents of a URL, *i.e.*, web-site page. ¶ [0055]. The use of persistent HTTP connections for intermediate devices to fetch content is further disclosed by Chauhan and is also suggested by an Internet standard, RFC 2616. *See* Ex. 8 ¶ [0007]; Ex. 12 at 29-31. It would have been obvious to incorporate such standard techniques into the Shribman '733 publication to avoid the handshaking overhead of having to open a new connection for every content request to the same web server, which is a well-known benefit of persistent connections as suggested by RFC 2616 itself. Ex. 3 ¶ 269.

7.4. SNQ Id: Obviousness of Claims 2-6, 8-10, 14-27, and 29 over the Shribman '733 publication in view of Liu and in further view of Sigurdsson and/or Chauhan

To the extent if any that the Shribman '733 publication is not deemed to fully anticipate claim 1, then Liu cures any such deficiency as discussed above. Thus, the same rationale as expressed above that would have made it obvious to have combined Liu with the Shribman '733 publication as to claim 1 would also apply with respect to each of claims 2-6, 8-10, 14-27,

and 29 as described in Section 7.3 with respect to the combination of the Shribman '733 publication with Sigurdsson and/or Chauhan.

7.5. SNQ Ie: Obviousness of Claims 11-12 over the Shribman '733 Publication in view of Bhatia

7.5.1. SNQ Ie (§ 103-Shribman '733 Publication + Bhatia)/ Claim 11

11. The method according to claim 9, wherein the client operating system is a mobile operating system.

As addressed above in connection with claim 9, the combination of the Shribman '733 publication and Chauhan render it obvious to implement claim 1 using a mobile device.

Bhatia further discloses wherein the client operating system is a mobile operating system, Ex. 17 ¶ [0018], lines 17-20 ("The mobile device 102, in illustrative embodiments, runs the ANDROID operating system."). Bhatia concerns a device layout wherein the mobile device acts as an intermediary to pass message packets from a device to which the mobile device is connected (such as a notebook computer or tablet), to a variety of application servers accessible to the mobile device over a broadband wide-area network (*e.g.*, Internet). It would have been obvious in view of Bhatia that a mobile operating system could be used to implement the claimed functionality of the client device, with predictable results. Since it would have been obvious to do so on a mobile device (as discussed in connection with claim 9), the incremental further provision of running a mobile *operating system* on the mobile device (as in claim 11) would clearly have also been obvious.

7.5.2. SNQ Ie (§ 103-Shribman '733 Publication + Bhatia)/ Claim 12

12. The method according to claim 11, wherein the mobile operating system is one out of Android version 2.2 (Froyo), Android version 2.3 (Gingerbread), Android version 4.0 (Ice Cream Sandwich), Android Version 4.2 (Jelly Bean), Android version 4.4 (KitKat)), Apple iOS version 3, Apple iOS version 4, Apple iOS version 5, Apple iOS version 6, Apple iOS version 7, Microsoft Windows® Phone version 7, Microsoft Windows® Phone version 8, Microsoft Windows® Phone version 9, and Blackberry® operating system.

See Ex. 2 at 299, citing Bhatia, a U.S. patent publication published prior to the earliest claimed priority date of the '614 patent. Bhatia teaches to use Android, without specifying the version. However, as of the claimed date of the invention (August 2013) using any one of the specified versions of Android, which is all the claim requires, would have been obvious, as a matter of current commercial availability and desire to address as large a market as possible. Since as discussed with regard to claims 9 and 11 it would have been obvious to implement claim 1 on a mobile device using a mobile operating system, the choice of such an OS, such as Android as in Bhatia, also would have been obvious.

7.6. SNQ If: Obviousness of Claims 11-12 over the Shribman '733 Publication in view of Liu and in further view of Bhatia

To the extent if any that the Shribman '733 publication is not deemed to fully anticipate claim 1, then Liu cures any such deficiency as discussed above. Thus, the same rationale as expressed above that would have made

it obvious to have combined Liu with the Shribman '733 publication as to claim 1 would also apply with respect to each of claims 11-12 as described in Section 7.5 with respect to the combination of the Shribman '733 publication with Bhatia.

7.7. SNQ Ig: Obviousness of Claim 28 over the Shribman '733 publication in view of Ebata

7.7.1. SNQ Ig (§ 103-Shribman '733 Publication + Ebata)/ Claim 28

28. The method according to claim 1, further comprising sending, by the client device, a physical geographical location to the first server, and wherein the physical geographical location corresponds to the actual physical geographical location of the client device.

The Shribman '733 publication (Ex. 6 ¶ [0088]) describes sorting peers by geographic proximity to the requesting client, reflecting the relevance of geographic location.²⁰

Ebata discloses selecting proxies based upon location so as to improve response speeds when requesting content. *See* Ebata, 4:23-45.

Like the Shribman '733 publication, Ebata concerns the selection of proxies to access a resource. *See* Ebata, Ex. 23, 4:23-28 (“a main object of the present invention to provide a comfortable working environment to a client in which only by specifying a logical node name of a server for pro-

²⁰ In the original prosecution, claim 28 was preliminarily indicated as allowable subject matter (Ex. 2 at 285), but the prosecution history suggests that the Examiner's intent may have been to allow claim 29 instead (Ex. 2 at 195). Ex. 2 at 290-91 suggests, on the other hand, that the Examiner withdrew the rejection of claim 28 based on disclosures in Chauhan. In any case, Ebata, cited herein, was not before the Examiner and is a strong reference on geographic tracking of content retrieval intermediaries.

viding a target service the client would like to reach, the most approximate proxy server to the client can be automatically selected”).

Ebata discloses storing a list of IP addresses of proxies and their related location information. *See* Ebata, Ex. 23, Fig. 8; 11:27-30 (“the SPS information list (625) includes the IP address, the location information and the load condition of each of the SPSs [service proxy servers] 2 and 7 distributively located on the network.”).

It would be obvious to associate each of the IP addresses in the list of IP addresses as taught in the Shribman ’733 publication with a corresponding geographical location, as disclosed in Ebata, as doing so would allow the client to select a proxy server based upon location so as to select the closest proxy and thus reduce response times, as suggested in Ebata. *See* Ebata, Ex. 23 at 3:49-52 (“[T]he user on the LAN can reuse the resource or the data cached in the proxy cache server that is a local server, so that the user may enjoy a comfortable response to the access.”). A POSITA would have a reasonable expectation of success of making such a combination since the Shribman ’733 publication teaches selection of a proxy according to certain criteria, which a POSITA understands could reasonably include geographic location, and since the combination is straightforward, yielding predictable results without significantly altering or hindering the functions performed by the system of the Shribman ’733 publication. *See* Ex. 3 ¶ 279. Specifically, this parallels the mechanism already described in the Shribman ’733 publication for making the agent selection based on “multiple factors, such as, for example, factoring the speed the reply by each agent,” or in other words, screening out agents that do not respond quickly, i.e., within a small amount of time (5 ms). *See* Ex. 6 ¶ [0084]; *see also* Ex. 6 at claim 29 (“wherein the list of one or more peer communication

devices includes only the peer communication devices that are the most beneficial to the requesting client communication device in terms of speed of receiving information from the peer communication devices”). A POSITA would understand that merely adding an additional or different attribute to the selection mechanism would not pose any kind of impediment for implementation. *See id.* Ex. 3 ¶ 279.

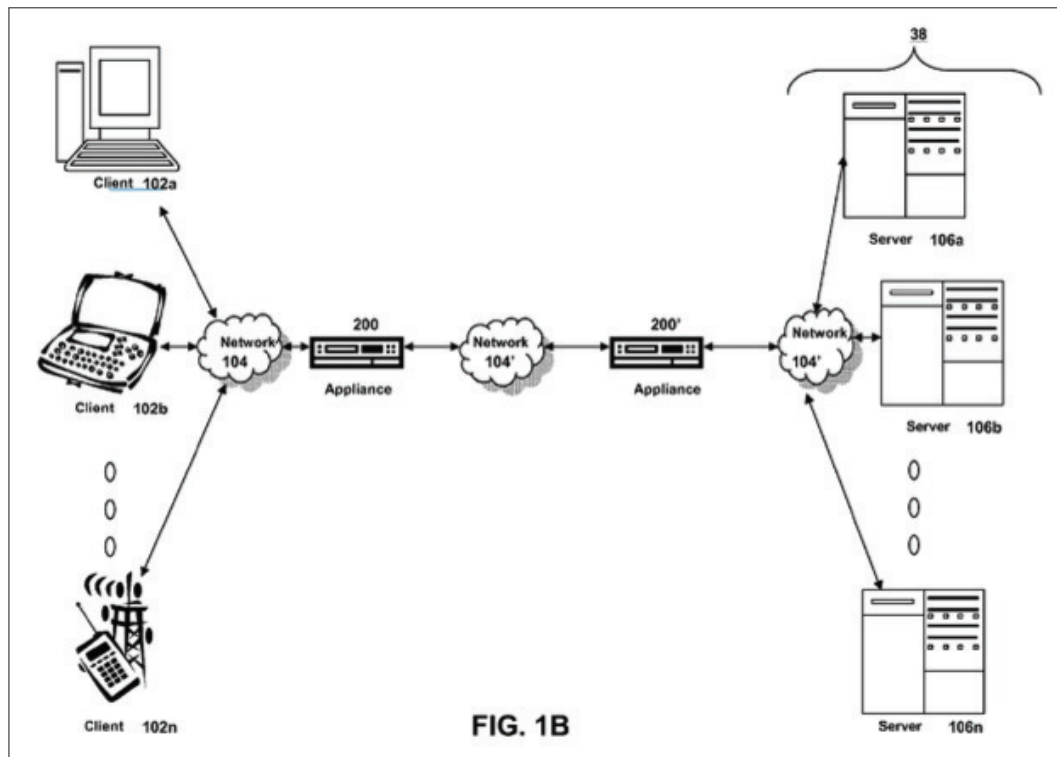
7.8. SNQ 1h: Obviousness of Claim 28 over the Shribman '733 publication in view of Liu and in further view of Ebata

To the extent if any that the Shribman '733 publication is not deemed to fully anticipate claim 1, then Liu cures any such deficiency as discussed above. Thus, the same rationale as expressed above that would have made it obvious to have combined Liu with the Shribman '733 publication as to claim 1 would also apply with respect to each of claim 28 as described in Section 7.7 with respect to the combination of the Shribman '733 publication with Ebata.

8. SNQ II: (a) ANTICIPATION OF CLAIMS 1-2, 4-12, 15-23, 25-26, AND 29 BY MITHYANTHA AND (b) OBVIOUSNESS OF CLAIMS 1-2, 4-12, 15-26, AND 28-29 OVER MITHYANTHA IN VIEW OF INTERNET STANDARDS AND GENERAL KNOWLEDGE OF A POSITA

Mithyantha discloses a system which, like the '614 patent, routes communications through plurality of interconnected nodes, where the nodes are associated with a state based on their utilization of a resource.

Figure 1B of Mithyantha illustrates an exemplary “network environment deploying multiple appliances 200.” Ex. 1 at 7:1-2:



Mithyantha, Fig. 1B

The network environment in Mithyantha comprises “one or more clients 102a-102n” that communicate with “one or more servers 106a-106n,” for example, when a web browser on a client 102 sends a request for a web page to a web server 106. *Id.* at 4:58-64, 6:52-53, 10:45-51, 11:1-24, 50-52, 23:55-58, Fig. 1B.

The “client 102 communicates with a server 106 via an appliance 200,” or, as in Figure 1B above, via “multiple appliances 200.” *Id.* at 4:64-65, 5:39-43, 7:1-18. The example of multiple appliances 200 can include multiple devices each having the minimum capabilities of appliance 200, such as appliances 200 and 200’ shown in Fig. 1B.²¹

²¹ The term “appliance 200” is used to refer to a class of appliance devices, of which appliance 200’ is an instance. *See* 7:1-18 (referring to “multiple appliances 200 ...including appliance 200’ ”). Further, with regard to terminology, in describing the disclosed functionality, Mithyantha uses the

Mithyantha itself further discloses that the appliance devices 200 may have interchangeable roles as clients and servers. Ex. 10 at 6:31-35:

In some embodiments, a client 102 also has the capacity to function as both a client node seeking access to applications on a server and as an application server providing access to hosted applications for other clients 102a-102n.

This means, in particular, that appliance 200' in Fig. 1B of Mithyantha may properly be regarded as a "client device" for purposes of the claims of the '614 patent, and that appliance 200 in the figure may properly be regarded as a "server" (and more particularly, the "first server") for purposes of the 614 patent claims.

Although Figure 1B includes exemplary images for client(s), appliances, and server(s), each device "may be deployed as and/or executed on any type and form of computing device, such as a computer, network device or appliance capable of communicating on any type and form of network." *Id.* at 13:65-14:2. Mithyantha discloses "computing device 100," a general-purpose computer with standard components and capabilities. *Id.* at 16:58-64; Fig. 1E, Fig. 1F. Computing device 100, as needed, can be a "desktop computer" or a "server," and can run consumer or server operating systems. *Id.* at 16:39-45, 57-64.

Appliance 200', also referred to as an "interface unit" or "gateway," can "act[] as a proxy or access server to provide access to the one or more servers 106." *Id.* at 5:31-33, 9:15-21, 53-55. "One or more appliances 200 may be located at any point in the network or network communications path between a client 102 and a server 106." *Id.* at 5:46-48.

terms "appliance 200" and "device 200" interchangeably. *E.g.*, compare Ex. 10 (Mithyantha) at 21:9, with same, 21:24.

Appliance 200 may thus be regarded as a “server,” and appliance 200’ to which it is connected via network 104’, may be regarded as a “client.” Network 104 and 104’ may both be the Internet. Ex. 10 5:3-7.

Client(s) 102 can connect to appliance(s)/device(s) 200—through a client data plane 602 and network 104—via “upstream router 700.” *Id.* at 53:5-19, 56:7-10, 17-27, Fig. 7A. Upstream router 700 can understand the various routing paths within the network and distribute traffic along desirable paths. *Id.* at 56:37-60, 57:11-21.

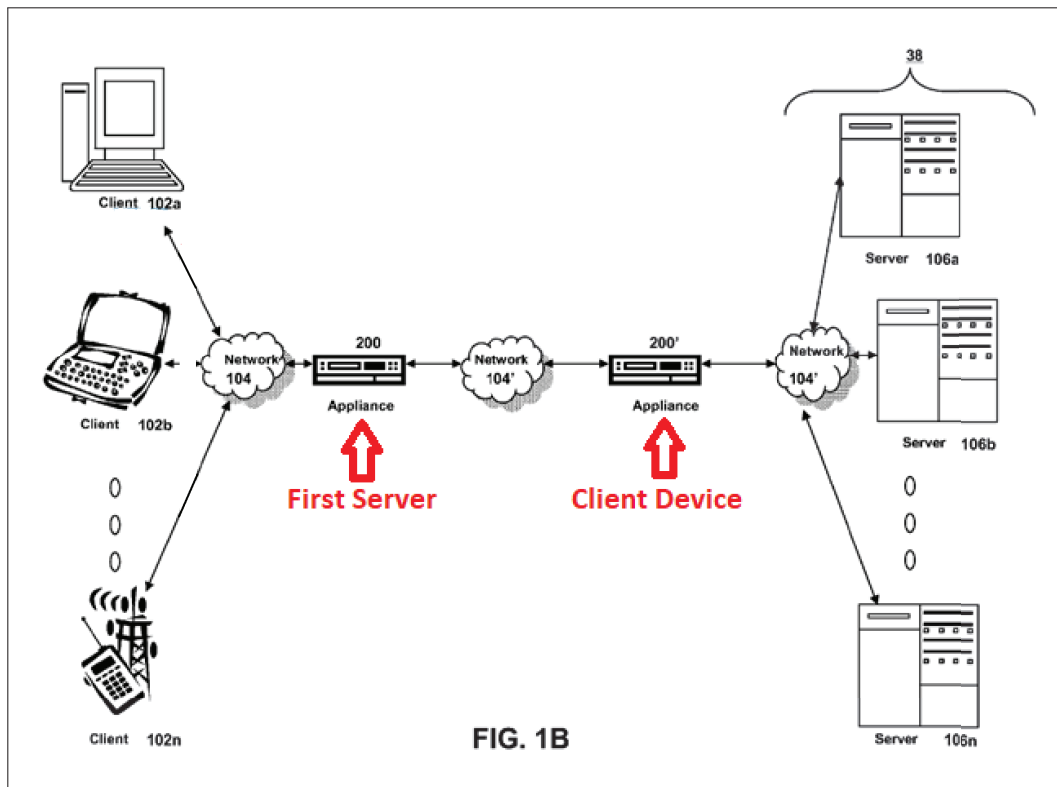
Furthermore, each appliance 200 may include “status monitor 704,” for “monitoring health,” such as “CPU usage or load, memory usage, bandwidth . . . or any other status of the device, vServer, network, or other entity.” *Id.* at 56:61-57:4.

As further explained below, Mithyantha fully anticipates claim 1 and a number of dependent claims of the ’614 patent. *See also* Ex. 3 ¶ 292.

8.1. SNQ IIa (§ 102)/Anticipation of Claims 1-2, 4-12, 15-23, 25-26, and 29 by Mithyantha

8.1.1. SNQ IIa (§ 102)/Claim 1

Requester compares Mithyantha against claim 1 on the basis of the following mapping of claim terms to the disclosure of Mithyantha:



Mithyantha Fig. 1B (With Mapping Annotation)

Client device: appliance/device 200' (or a virtual server 702 running on such a device)

First server: appliance/device 200 (between client(s) 102 and appliance 200')

Resource: one of CPU usage, memory usage, or bandwidth

Criterion: the amount of usage (threshold) of the resource

First Identifier: IP address associated with the client device

First state: active/available

Second state: inactive/unavailable

Mithyantha (§ 102) vs. Preamble [1.P]—“A method for use with a resource associated with a criterion in a client device that communi-

cates with a first server over the Internet, the client device is identified in the Internet using a first identifier and is associated with first and second state according to a utilization of the resource, the method comprising”

Examining the preamble clause-by-clause:

A method for use with a resource associated with a criterion in a client device . . .

Mithyantha discloses a method that is used with a resource associated with a criterion in a client device. This concerns the “status monitor” incorporated in each appliance device 200.

First, appliance/device 200’ of Mithyantha may properly be considered a “client device” for purposes of the claims. Mithyantha itself expressly contemplates appliance/device 200 operating in a client role. Ex. 10 at 6:31-35. In any case, in accordance with “client” and “server” roles as described in the ’614 patent, appliance/device 200 acts as a client to any of servers 106a-106n. See discussion of client-server roles as contemplated in the ’614 patent, in Section 3.1 above.

The client devices 102 of Mithyantha incorporate a “status monitor” for “monitoring the health . . . of the device, . . . or other entity.” Ex. 10 at 56:61-57:4. The status monitor concerns resources associated with the health of the device, which the monitor compares with relevant criteria.

Per the disclosure, *e.g.*, Ex. 10 at 23:12-15, “Health monitoring program 216 is used to monitor, check, report and ensure that network systems are functioning properly and that users are receiving requested content over a network. Health monitoring program 216 comprises one or more programs, services, tasks, processes or executable instructions to

provide logic, rules, functions or operations for monitoring any activity of the appliance 200 . . . As such, the health monitoring program 216 may call any application programming interface (API) to determine a state, status, or health of any portion of the appliance 200.”

If “a monitored status or value exceeds a threshold,” the device may be withdrawn from the upstream server’s list of client devices. Ex. 10 at 57:11-19.

As disclosed in Mithyantha, the “resource” may be “CPU usage or load, memory usage, bandwidth . . . or any other status” in a client device (such as Mithyantha’s appliance/device 200). Ex. 10 at 56:61-57:4. The “criterion” as disclosed in Mithyantha is a threshold, such as where “a monitored status or value exceeds a threshold, such as a CPU utilization rate past a threshold for a predetermined time.” *Id.* at 57:4-14.

Thus, there is express disclosure in Mithyantha for a method in accordance with this preamble language.

. . . that communicates with a first server over the Internet . . .

As noted in Fig. 1B (above), appliance/device 200’ (client device) in Mithyantha communicates with appliance/device 200 (first server) over Network 104’, which may be the Internet (Ex. 10 at 5:1-7).

Appliance/device 200 may be the claimed ‘first server’ because appliance/device 200 functions as a server in the disclosed system. In particular, appliance/device 200 functions as a server to retrieve content for clients 102a-102n, fully qualifying as a “server” as that term is used in the ‘614 patent. See Ex. 1 at 6:27-42.

Mithyantha thus discloses a client device that communicates with a first server over the Internet.

... identified in the Internet using a first identifier ...

Mithyantha discloses that each device 200 (a class of devices that includes the 200' client device per this claim) "may execute a virtual server or vServer 702a-702n," which may be identified by an IP (Internet Protocol) address. Ex. 10 at 56:17-29. Per the governing standards of the Internet, *e.g.*, Ex. 22, RFC 791 (§ 3.2 at 23), a device's IP address is what identifies it on the Internet. *See* Ex. 3 ¶ 305.

Mithyantha thus discloses this limitation.

... and is associated with first and second state according to a utilization of the resource ...

"Client device" appliance/device 200' "may comprise a status monitor 704a-704m, referred to generally as status monitor(s) 704," for monitoring its own health and the health of devices on the network. Ex. 10 at 56:61-57:4. "Monitoring health may comprise monitoring CPU usage or load, memory usage, bandwidth ... or any other status." *Id.* "[A] status monitor of a device may periodically poll other devices for health status" and "may determine that a monitored status or value exceeds a threshold, such as a CPU utilization rate past a threshold for a predetermined time." *Id.* at 57:4-14. The disclosure specifically refers to the results of this monitoring as reflecting the "state" of the device. *Id.* at 23:12-36 ("[H]ealth monitoring program 216 may call any application programming interface (API) to determine a *state* ... of any portion of the appliance 200.") (emphasis added).

Mithyantha thus discloses that the client device is associated with first and second state according to a utilization of the resource, and with that, it is thus seen that Mithyantha discloses the entire preamble. Ex. 3 ¶ 308.

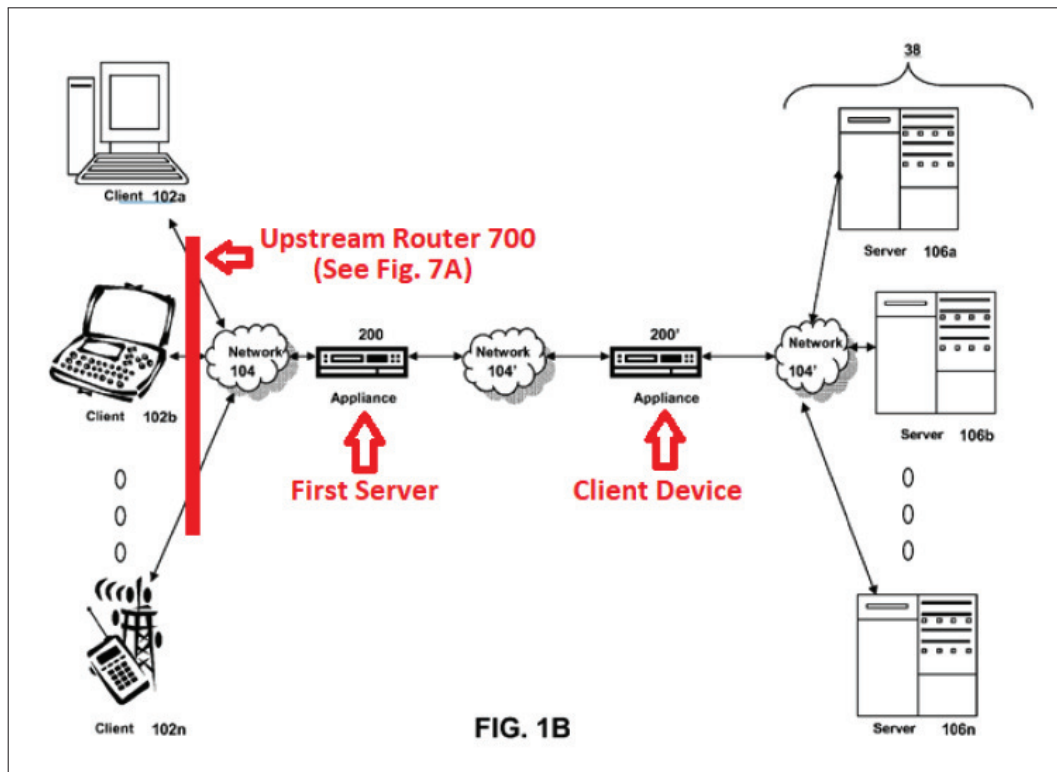
Mithyantha (§ 102) vs. Claim Step [1.1]—“initiating, by the client device, communication with the first server over the Internet in response to connecting to the Internet, the communication comprises sending, by the client device, the first identifier to the first server over the Internet”

Addressing this limitation clause-by-clause:

initiating, by the client device, communication with the first server over the Internet . . .

initiating, by the client device—Mithyantha discloses the client device initiating a communication. It states in this regard that appliance/device 200’ sends a first identifier (the IP address associated with the appliance/device 200’) to an upstream router 700 over networks 104/104’, which may both be the Internet. *See* Ex. 10 at 55:61-56:60.

. . . communication with the first server over the Internet—This initiated communication is “with the first server” and “over the Internet.” Appliance/device 200’ (client device) communicates through appliance/device 200 (first server) with upstream router 700. Ex. 10 at Fig. 1B, 56:17-45, 25:24-31 (an IP address is a network identifier):



Mithyantha Fig. 1B (Annotated)

Since the communication by client device 200' with upstream router 700 is over the Internet and through appliance device 200, this necessarily entails the client device (appliance device 200') communicating with the intermediate devices in this chain of communication, *i.e.*, appliance device (first server) 200. Ex. 3 ¶ 312. Moreover, Mithyantha specifically discloses embodiments in which each appliance/device 200 runs vServer 702, which has the capability for "receiving, intercepting, processing, and/or forwarding packets to and from nodes of the cluster, servers, clients, or any combination of devices." See Ex. 10 at 56:17-36. A POSITA would understand that in embodiments using such a vServer, the communication between client device 200' and upstream router goes through and is handled by vServer 202 running on, *i.e.*, within, appliance device 200, such that the vServer, and this appliance device 200' (first server) would receive and

forward the IP address of appliance device 200' (first client device). Ex. 3 ¶ 312.

Thus, the limitation that the client device communicates with the first server over the Internet is met by Mithyantha's disclosure that the communication by the client device over the Internet goes by way of the first server, and is thus is necessarily also *with* the first server.

...in response to connecting to the Internet

Intermediary devices in Mithyantha advertise "a corresponding IP address ... as devices become active or inactive." *Id.* at 58:38-61, Fig. 7C. Fig. 7C "is a flow chart of an embodiment of a method for using multi-path routing for traffic distribution in a cluster environment." *Id.* at 4:17-19. The first step shown in Fig. 7C is step 740, "Advertise address of vServer and metric n." The Mithyantha specification states: "at Step 740, each intermediary device of a cluster comprising a plurality of intermediary devices may advertise, via a routing protocol to a router, a corresponding IP address of a virtual server executing on each intermediary device and one or more connection metrics having predetermined values." *Id.* at 58:41-45. The context of the disclosure reflects that in some embodiments the flow of steps represented in Fig. 7C is executed on startup of the appliance, upon establishing a network connection, *i.e.*, upon connecting to the Internet. Ex. 3 ¶ 314.

In addition, a device re-advertises its route upon return to the network (and thus when it again connects to the Internet, and therefore "in response to connecting to the Internet"). Ex. 10 at 57:32-61. For example, "client device" appliance/device 200' may leave the network after losing connection to the Internet. *See, e.g., id.* at 57:36-39, 57:62-58:2. Upon regaining its connection, appliance/device 200' re-advertises

its route (which, at a minimum, includes its identifier). *Id.* at 57:32-61, claim 10; Ex. 3 ¶ 315.

Both the advertisement and the re-advertisement will necessarily be sent, over Internet 104', to "first server" appliance/device 200 before arriving at the final destination, upstream router 700. Ex. 10 at Fig. 1B, Fig. 7A.

Upstream router 700 maintains a routing table of the identifiers of the intermediary devices that comprise the network. *Id.* at 57:19-21, 57:36-47, 58:22-26. Further, a POSITA would understand that devices communicating over the Internet would send an identifier to facilitate communication. *See, e.g., id.* at 2:44-62; Ex. 3 ¶ 317.

The annotated version of Mithyantha's Fig. 1B shown above reflects that in the Figure 1B multi-proxy embodiment, "client device" appliance/device 200' would necessarily send the first identifier to "first server" appliance/device 200 before it arrived at upstream router 700, which is placed between client(s) 102 and the first server (appliance/device 200) in the network path. Ex. 10 at 53:5-19, 56:7-10, 17-27, Fig. 1B, Fig. 7A. In this regard, as noted above, Mithyantha further discloses embodiments in which each appliance/device 200 runs vServer 702, which specifically has the capability for "receiving, intercepting, processing, and/or forwarding packets to and from nodes of the cluster, servers, clients, or any combination of devices" *See id.* at 56:17-36.

Thus, Mithyantha discloses that the client device initiates communication with the first server, as claimed, "in response to connecting to the Internet."

...the communication comprises sending, by the client device, the first identifier to the first server over the Internet

The express disclosure is that appliance device 200' (client device) sends its IP address to upstream router 700. *See* Ex. 10 at 55:61-56:60. This communication is also disclosed to be via network 104/104' (which can be Internet) connections *through* appliance device 200 (first server), and therefore the IP address must also be communicated to the first server. Ex. 3 ¶ 320.

Mithyantha (§ 102) vs. Claim Step [1.2]—“when connected to the Internet, periodically or continuously determining whether the resource utilization satisfies the criterion”

“Client device” appliance/device 200’ “may comprise a status monitor 704a-704n, referred to generally as status monitor(s) 704,” for monitoring its own health and the health of devices on the network. Ex. 10 at 56:61-57:4. “Monitoring health may comprise monitoring CPU usage or load, memory usage, bandwidth . . . or any other status.” *Id.* It “may comprise . . . [a] service, daemon, routine, or other executable logic for monitoring health of one or more devices, vServers, [etc.].” *Id.* “[A] status monitor of a device may periodically poll other devices for health status” and “may determine that a monitored status or value exceeds a threshold, such as a CPU utilization rate past a threshold for a predetermined time.” *Id.* at 57:4-14.

Status monitor 704 functions when “connected to the Internet,” as it monitors network devices connected via the Internet. *Id.* at 5:3-7, 56:67-57:4.

A similar “monitoring agent 197” that “measures and monitors the memory, CPU and disk usage and performance of the appliance 200” and other devices on the network is also disclosed. *Id.* at 11:46-50, 62-66, 27:65-67.

Mithyantha discloses this limitation. Ex. 3 ¶ 324.

Mithyantha (§ 102) vs. Claim Step [1.3]—“responsive to the determining that the utilization of the resource satisfies the criterion, shifting to the first state or staying in the first state”

Mithyantha states:

“[S]tatus monitor 704 may determine that a monitored status or value exceeds a threshold, such as a CPU utilization rate past a threshold for a predetermined time. Responsive to the determination, the status monitor 704 may direct the vServer 702 of the device to withdraw its advertised route from the upstream router 700. This may be done to reduce or eliminate incoming traffic while the device resolves any issues or errors, to allow the device to reboot, or any other such reason. Once received, the router 700 may update its multipath routing table and continue routing traffic 20 to other, active nodes of the cluster.”

Ex. 10 at 57:11-21. *See also* Ex. 10 at 59:13-50.

The “determination” referenced in the above quote reflects a “state” of the appliance device or a vServer running on that device. The determination that monitored status or value exceeds a specified threshold results in a determination that reflects an unavailable state. Per the above-quoted disclosure, if the monitored status exceeds the specified threshold, the status monitor may direct the vServer the withdraw its advertised route, which, certainly in the broadest reasonable interpretation of the claim language, constitutes a change of state. Conversely, a determination that the status or value does not exceed the threshold reflects an available state. Thus, the device stays in an available state until such time conditions cause it to shift to an unavailable state.

Appliance/device 200’ may shift between the first and second state when, for example, appliance/device 200’ exceeds a threshold and there-

after returns to utilization below the threshold: “if the unavailable node returns, it may re-advertise its route . . . such that the router 700 may begin including it in load balancing and multipath routing without requiring all devices to re-advertise their routes.” *Id.* at 57:57-61.

Mithyantha discloses this limitation. Ex. 3 ¶ 328.

Mithyantha (§ 102) vs. Claim Step [1.4]—“responsive to the determining that the utilization of the resource does not satisfy the criterion, shifting to the second state or staying in the second state”

Mithyantha’s express disclosures discussed directly above regarding the second and third claim steps, and the vServer’s withdrawal of an advertised route when a monitored status or value exceeds a threshold, incorporated here, satisfy this claim limitation as well.

Mithyantha discloses this limitation. Ex. 3 ¶ 330.

Mithyantha (§ 102) vs. Claim Step [1.5]—“responsive to being in the first state, receiving, by the client device, a request from the first server”

“Client device” appliance/device 200’, when in the first state, receives requests from client(s) 102, via “first server” appliance/device 200. Ex. 10 at 57:32-61, Fig. 1B, Fig. 7A. Such requests may include requests from a web browser on client(s) 102, sent via upstream router 700, appliance/device 200, and appliance/device 200’, to web server(s) 106.

This is “responsive to being in the first [available] state,” insofar as the state-determination mechanism in Mithyantha, by which a device may determine that it is unavailable, is designed to enable the upstream router 700 to “withdraw” the unavailable device from the set of routes to which

tasks will be allocated, and “and continue routing traffic 20 to other, active [i.e., available] nodes of the cluster.” See Ex. 1 at 57:14-21; Ex. 3 ¶ 332.

Mithyantha discloses this limitation. Ex. 3 ¶ 333.

Mithyantha (§ 102) vs. Claim Step [1.6]—“performing a task, by the client device, in response to the receiving of the request from the first server”

Mithyantha’s express disclosures discussed directly above regarding claim step [1.5] (including, *e.g.*, requests from a web browser), incorporated here, satisfy this claim limitation. The “task” performed is further described below regarding claim steps [1.7]-[1.11].

Mithyantha discloses this limitation. Ex. 3 ¶ 335.

Mithyantha (§ 102) vs. Claim Step [1.7]—“wherein the method is further configured for fetching over the Internet a first content identified by a first content identifier from a web server that is distinct from the first server, and the task comprising”

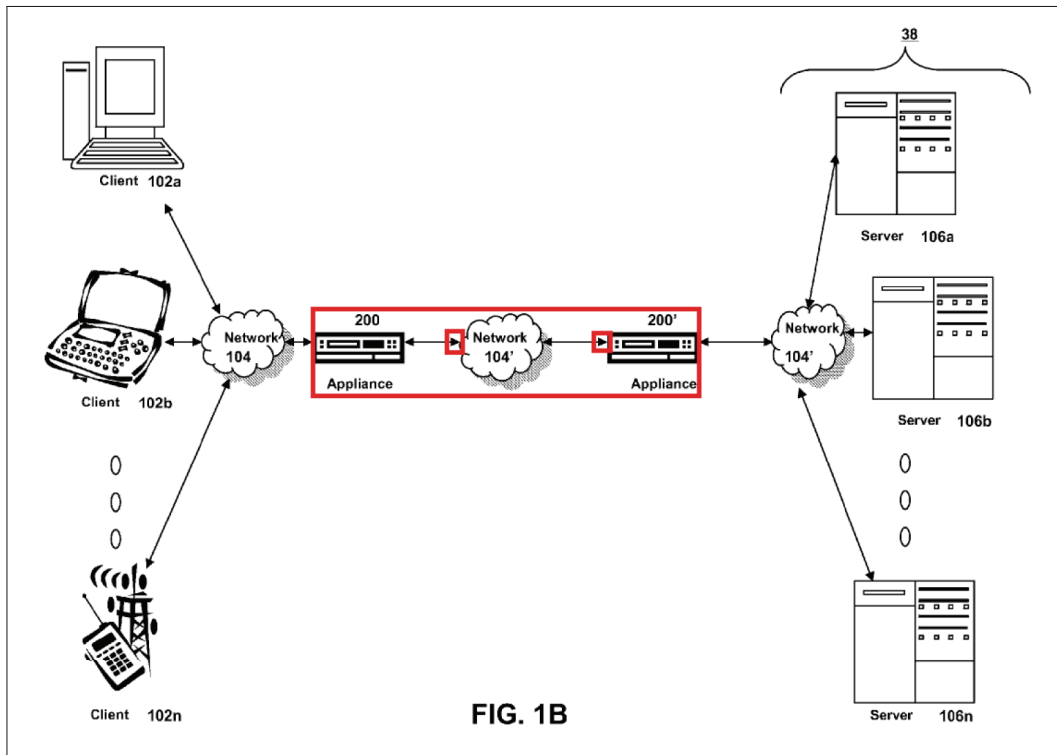
Mithyantha discloses a system that can be used to fetch web content from a web server over the Internet. An HTTP request for web content can be created at a “web browser” on client 102. *Id.* at 10:45-51, 60-62. That initial HTTP request is sent to upstream router 700 that directs the request to “first server” appliance/device 200 and thereafter “client device” appliance/device 200’. *Id.* at 4:64-65, 7:1-18, 56:7-23, Fig. 1B, Fig. 7A. “Client device” appliance/device 200’, acting “as a proxy or access server,” then forwards the HTTP request to “web server” 106. *Id.* at 6:52-53, 9:15-17, 53-55, 11:13-18, 23:55-58. Each of these requests are routed via Internet networks 104 and 104’ using “any TCP/IP based protocol,” including HTTP. *Id.* at 5:3-7, 19:4-8, 21:21-38, 28:55-58.

The “first content” and “first content identifier,” as well as the reminder of the method steps that “comprise” this claim element, are discussed in detail below.

Mithyantha discloses this limitation. Ex. 3 ¶ 338.

Mithyantha (§ 102) vs. Claim Step [1.8]—“receiving, by the client device, the first content identifier from the first server”

As explained in Section 8.1 above, Mithyantha discloses a network of devices capable of handling HTTP web requests for web pages sent between a web browser and a web server. *See, e.g.*, Ex. 10 at 4:58-64, 6:52-53, 10:45-51, 11:1-24, 11:50-52, 23:55-58. This claim limitation is met when “client device” appliance/device 200’ receives the HTTP web request from “first server” appliance/device 200. Ex. 10 at 3:45-47, 4:64-65, 7:1-18, 9:15-17, Fig. 1B. Annotated Figure 1B shows this step:



Annotated Figure 1B from Mithyantha

As the '614 patent acknowledges, "HTTP resources are identified and located on the network by Uniform Resource Identifiers (URIs) or, more specifically, Uniform Resource Locators (URLs)." Ex. 1 at 5:38-41. A POSITA would understand that the HTTP web browser requests disclosed in Mithyantha, *see e.g.*, Ex. 10 at 10:45-61, 11:50-52, 23:57-58, would include a content identifier (*e.g.*, a URL) that identifies first content (*e.g.*, a web page). Ex. 3 ¶ 340.

Mithyantha discloses this limitation. *Id.* at ¶¶ 102-04.

Mithyantha (§ 102) vs. Claim Step [1.9]—"sending, by the client device, the first content identifier to the web server"

As explained in Section 8.1, after receiving the first content identifier, "client device" appliance/device 200', serving as proxy, sends the HTTP request (containing the first content identifier, *e.g.*, URL) to any of "web servers" 106a-n. Ex. 10 at 4:64-65, 6:52-53, 9:15-17, 53-55, 23:57-58.

A POSITA would understand that HTTP web browser requests disclosed in Mithyantha, *see e.g.*, *id.* at 10:45-61, 11:50-52, 23:57-58, include a content identifier (*e.g.*, a URL) identifying first content (*e.g.*, a web page). Ex. 3 ¶ 343.

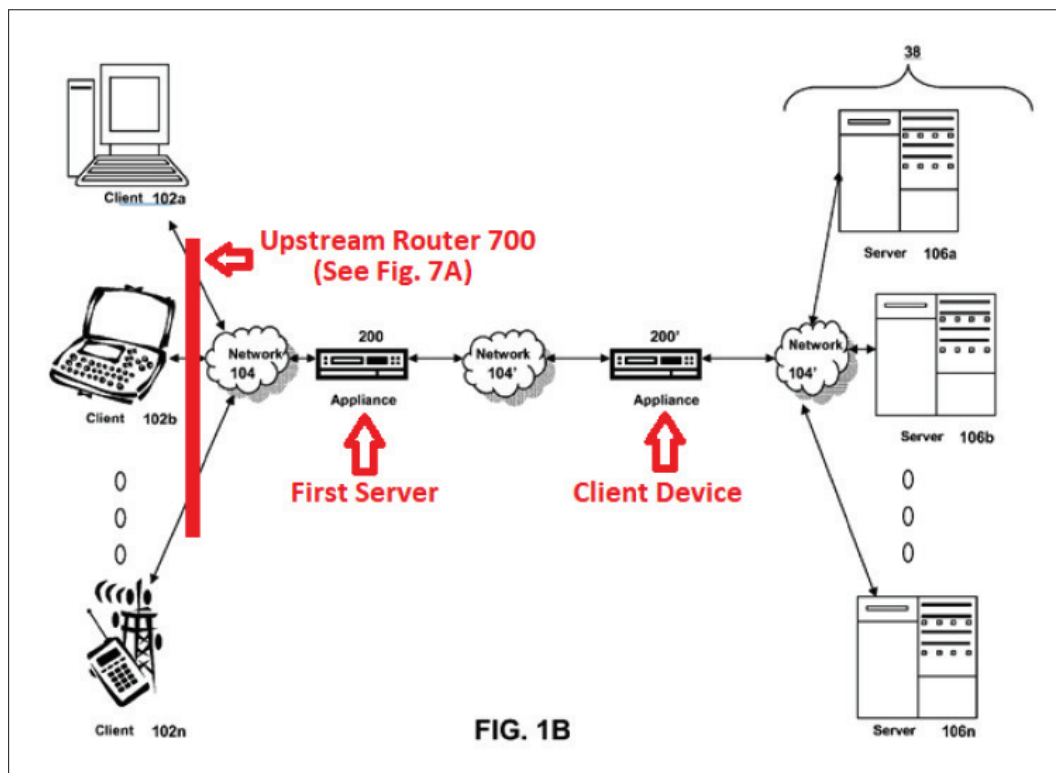
Mithyantha thus discloses this limitation. *Id.* at ¶¶ 105-07.

Mithyantha (§ 102) vs. Claim Step [1.10]—"receiving, by the client device, the first content from the web server in response to the sending of the first content identifier"

As further explained in Section 8.1, after the client device sends the first content identifier (*e.g.*, URL) to any of "web servers" 106a-n, the "client device" appliance/device 200' receives, in response and still serving as proxy, the first content (*e.g.*, a web page) from the "web server." Ex. 10

at 4:64-65, 9:15-17, 11:50-52, 20:9-16, 21:21-38, 53:26-28, 56:17-23.

Again, annotated Figure 1B shows this step:



Mithyantha Fig. 1B (Annotated)

As the '614 patent acknowledges, “[T]he primary purpose of a web browser is to bring information resources to the user” Ex. 1 at 20:4-27, 63:26-29 (“the first content may be a web-site, a web-page, or a URL”). A POSITA would understand that the HTTP web browser requests disclosed in Mithyantha, *see e.g.*, Ex. 10 at 10:45-61, 11:50-52, 23:57-58, would cause a web server to respond with first content (*e.g.*, a web page) to be delivered to the web browser where the HTTP request originated. Ex. 3 ¶ 346.

Mithyantha thus discloses this limitation. *Id.* at ¶¶ 108-10.

Mithyantha (§ 102) vs. Claim Step [1.11]—“sending, by the client device, the received first content to the first server”

As further explained in Section 8.1, after the client device receives the first content (*e.g.*, a web page), the client device appliance/device 200', still serving as proxy, sends that content to the first server appliance/device 200 so that the first content (*e.g.*, a web page) can be forwarded to the originator of the HTTP request, the web browser of client 102. Ex. 10 at 4:64-65, 7:1-18, 9:15-17, 53:26-28, 56:17-23, Fig. 1B. Annotated Figure 1B (above) also shows this step.

A POSITA would understand that the HTTP web browser requests disclosed in Mithyantha, *see e.g.*, Ex. 10 at 10:45-61, 11:50-52, 23:57-58, would cause a web server to respond with first content (*e.g.*, a web page) to be delivered to the web browser where the HTTP request originated. Ex. 3 ¶ 349.

Mithyantha discloses this limitation.

8.1.2. SNQ IIa (§ 102)/Claim 2

2. The method according to claim 1, wherein the determining is performed by the client device.

Mithyantha discloses that “client device” appliance/device 200’ “may comprise . . . status monitor(s) 704.” Ex. 10 at 56:61-57:4, Fig. 7A. Status monitor 704 satisfies the “determining” limitation of claim 1 via the monitoring of resource utilization, including CPU, memory, and bandwidth utilization. “[S]tatus monitor 704 may determine that a monitored status or value exceeds a threshold, such as a CPU utilization rate past a threshold for a predetermined time.”

Mithyantha thus discloses this limitation. Ex. 3 ¶ 352.

8.1.3. SNQ IIa (§ 102)/Claim 4

4. The method according to claim 1, wherein the communication by the client device with the first server is based on, or is according to, TCP/IP protocol or connection.

“Client device” appliance/device 200’ communicates with “first server” appliance/device 200 via network 104’. Ex. 10 at 7:1-18, Fig. 1B. Network 104’ can be the Internet, over which appliance/device 200’ and 200 using “any TCP/IP based protocol.” *Id.* at 5:3-7, 19:4-8, 21:21-38, 28:55-58, Fig. 1B.

Furthermore, appliance/device 200’ and 200 each “comprises one network stack 267, such as a TCP/IP based stack, for communicating with the client 102 and/or the server 106.” *Id.* at 19:4-6. Appliance/device 200’ and 200 also contain compression logic, *id.* at 19:27-30, Fig. 2A, which “compresses bidirectionally ... any TCP/IP based protocol.” *Id.* at 21:24-27. Similarly, client 102’s network stack “may comprise a transport control protocol (TCP) over the network layer protocol of the internet protocol (IP).” *Id.* at 28:31-47.

Thus, Mithyantha discloses that communications between appliance/device 200’ and client(s) 102, passing through appliance/device 200, may be based on the TCP/IP protocol.

Mithyantha discloses this limitation. Ex. 3 ¶ 356.

8.1.4. SNQ IIa (§ 102)/Claim 5

5. The method according to claim 4, further comprising establishing a connection with the first server, and wherein the communication with the first server is over the established connection, and wherein the communicating by the client device with the first server uses

TCP, and wherein the connection is established by performing ‘Active OPEN’ or ‘Passive OPEN’.

Claim 5 adds that the establishment of the TCP connection be performed by “Active OPEN” or “Passive OPEN” approaches. The ’614 patent acknowledges that “Active OPEN” and “Passive OPEN” are standard TCP establishment approaches. Ex. 1 at 2:41-65; Ex. 28 § 2.7. A POSITA would understand that the disclosure of TCP/IP, as described directly above, teaches “Active OPEN” and “Passive OPEN” as the only possibilities, and necessarily encompasses these standard means of connecting. Ex. 3 ¶ 357.

Mithyantha discloses this limitation. *Id.* at ¶¶ 122-24.

8.1.5. SNQ IIa (§ 102)/Claim 6

The method according to claim 5, wherein the communication by the client device with the first server is based on, or is according to, a Virtual Private Network (VPN) and the established connection is using a tunneling protocol.

Appliances/devices 200’ and 200 can “provide[] a secure virtual private network connection from a first network 104 of the client 102 to the second network 104’ of the server 106, such as an SSL VPN connection,” and therefore can operate as tunneling devices. Ex. 10 at 9:18-21. Indeed, the ’614 patent specifically discloses recognizes the use of tunneling protocols to provide a VPN connection. *See, e.g.*, Ex. 1 at 29:25-30:58 (“Virtual Private Networks (VPNs) are point-to-point connections across a private or public network, such as the Internet. A VPN client typically uses special TCP/IP-based protocols, called tunneling protocols to make a virtual call to a virtual port on a VPN server.”). As such, in Mithyantha, “the encryp-

tion engine 234” on appliances/devices 200’ and 200 “uses a tunneling protocol to provide a virtual private network” between client and server. Ex. 10 at 21:13-16. And “the vServer 275” on appliance/device 200’ and 200 can perform “SSL VPN” *Id.* at 24:3-5, Fig. 2B.

Mithyantha discloses this limitation. Ex. 3 ¶ 360.

8.1.6. SNQ IIa (§ 102)/Claim 7

7. The method according to claim 1, wherein the steps are sequentially executed.

Mithyantha discloses the sequential execution of claim 1’s steps.

Appliance/device 200’ must send its identifier to upstream router 700, via appliance/device 200, for the router to add its advertised path to the routing table. *See* Section 8.1.1.

Once connected to the network, status monitor 704 (and/or monitoring agent 197) periodically or continuously determines resource utilization. *See id.*

In the event appliance/device 200’ leaves the network, and thereafter returns, there will be a shift from first state, to second state, and back to first state. *See id.*

Following these shifts, appliance/device 200’ may receive a request from the first server, and thereafter perform the Internet content fetching tasks, in sequential order. *See id.*

Mithyantha discloses this limitation. Ex. 3 ¶ 366.

8.1.7. SNQ IIa (§ 102)/Claim 8

8. The method according to claim 1, wherein the first identifier comprises an IP address that is in IPv4 or IPv6 form.

As discussed in Section 8.1.1, incorporated here, Mithyantha discloses that a first identifier (the IP address associated with appliance/device 200') is sent via the "first server" to upstream router 700 for traffic routing. Mithyantha discloses routing via "flow distributor 550," which "can comprise a Receive Side Scaler (RSS) or Receive Side Scaling (RSS) module 560" located on "any type and form of" device. *Id.* at 43:11-25. The RSS module "can apply ...TCP/IPv4, TCP/IPv6, IPv4, and IPv6 headers." *Id.* at 47:20-33. Thus, the first identifier may comprise an IP address in IPv4 or IPv6 form.

Furthermore, IPv4 and IPv6 are the only two supported IP address formats on the Internet, and thus, Mithyantha disclosing use of an IP address necessarily discloses uses of such formats. Ex. 3 ¶ 368.

Mithyantha thus discloses this limitation. Ex. 3 ¶ 369.

8.1.8. SNQ IIa (§ 102)/Claims 9-12

9. The method according to claim 1, wherein the client device is further storing, operating, or using, a client operating system.

10. The method according to claim 9, wherein the client operating system consists or, comprises of, or is based on, one out of Microsoft Windows 7, Microsoft Windows XP, Microsoft Windows 8, Microsoft Windows 8.1, Linux, and Google Chrome OS.

11. The method according to claim 9, wherein the client operating system is a mobile operating system.

12. The method according to claim 11, wherein the mobile operating system is one out of Android version 2.2 (Froyo), Android version 2.3 (Gingerbread), Android version 4.0 (Ice Cream Sandwich), Android

Version 4.2 (Jelly Bean), Android version 4.4 (KitKat)), Apple iOS version 3, Apple iOS version 4, Apple iOS version 5, Apple iOS version 6, Apple iOS version 7, Microsoft Windows® Phone version 7, Microsoft Windows® Phone version 8, Microsoft Windows® Phone version 9, and Blackberry® operating system.

“[T]he operating system [of appliance/device 200] may be any type and/or form of Unix operating system,” as well as any version of “Microsoft® Windows operating systems . . . Unix and Linux operating systems . . . Mac OS® for Macintosh computers . . . any operating systems for mobile computing devices or network devices, or any other operating system capable of running on the appliance 200 and performing the operations.” Ex. 10 at 18:41-56, Fig. 2A. Additionally, appliance/device 200’ may run on computing device 100, *id.* at 14:3-5, which “can be running any operating system” and “any operating systems for mobile computing devices.” *Id.* at 16:30-50, Fig. 1E. Though Mithyantha teaches the use of “any operating systems for mobile computing devices,” without specifying the mobile operating system or version thereof, as of the claimed date of the invention (August 2013) using any one of the specified versions of Android, Apple iOS, Microsoft Windows Phone, or Blackberry operating system, which is all the claim requires, would have been obvious, as a matter of current commercial availability and desire to address as large a market as possible.

Mithyantha discloses these limitations. Ex. 3 ¶ 371.

8.1.9. SNQ IIa (§ 102)/Claims 15-16

15. The method according to claim 1, wherein the client device comprises, or consists of, a portable or mobile device.

16. The method according to claim 15, wherein the mobile device comprises a smartphone.

Mithyantha discloses “client device” appliance/device 200’ that may run on computing device 100, Ex. 10 at 14:3-5, which “can be any . . . hand-held computer, mobile telephone, any other computer,” including a Treo smartphone. Ex. 10 at 16:53-64.

Mithyantha thus discloses these limitations. Ex. 3 ¶ 373.

8.1.10. SNQ IIa (§ 102)/Claim 17

The method according to claim 1, for use with a set threshold value, and wherein the criterion is satisfied when the resource utilization is above or below the threshold.

As discussed in Section 8.1, “status monitor 704 may determine that a monitored status or value exceeds a threshold, such as a CPU utilization rate past a threshold for a predetermined time.” Ex. 10 at 57:11-14, 2:15-19, 3:4-8, claim 4.

Mithyantha discloses this limitation. Ex. 3 ¶ 375.

8.1.11. SNQ IIa (§ 102)/Claims 18-23

18. The method according to claim 1, wherein the resource comprises, or consists of, a hardware component in the client device.

19. The method according to claim 18, wherein the hardware component comprises, or consists of, a processor or Central Processing Unit (CPU) operation in the client device.

20. The method according to claim 19, wherein the resource utilization is based on, or comprises, the processor or CPU time of executing

one or more threads or processes, wherein the resource utilization is based on, or comprises, the processor or CPU idling time, or wherein the resource utilization is based on, or comprises, the processor or CPU executing a system idle process.

21. The method according to claim 18, wherein the hardware component comprises, or consists of, a memory in the client device, and wherein the resource utilization is based on, or comprises, an amount of used or unused location or space of the memory.

22. The method according to claim 1, wherein the resource comprises, or consists of, input or output capability.

23. The method according to claim 22, wherein the resource comprises, or consists of, communication bandwidth of communication with another device over the Internet.

Claims 18-23 all concern implementations where the resource being monitored is a hardware component.

As discussed in Section 8.1, “status monitor 704 may determine that a monitored status or value exceeds a threshold, such as a CPU utilization rate past a threshold for a predetermined time.” Ex. 10 at 57:11-14, 2:15-19, 3:4-8, claim 4. “Monitoring health may comprise monitoring CPU usage or load, memory usage, bandwidth ... or any other status of the device, vServer, network, or other entity.” *Id.* at 56:63-57:4. Similarly, “the monitoring agent 197 measures and monitors,” among other things, “the memory, CPU and disk usage and performance of the appliance 200,” including bandwidth utilization. *Id.* at 27:65-67; 11:46-12:7, 12:12-19, 45-49, 13:3-21, 34-44, 33:4-7.

Thus, the “resource” of claim 1 may comprise a hardware component (*e.g.*, CPU, *id.* at 14:15-18, memory, *id.* at 14:28-44, and/or network interfaces/input/output devices, *id.* at 15:26-39, 16:18-26, in appliance/device 200’, *id.* at 13:65-14:7, Fig. 1E, Fig. 1F. Or the “resource” of claim 1 may comprise input or output capability, *id.* at 13:65-14:7, 15:26-39, 16:18-26, Fig. 1E, Fig. 1F, including bandwidth of communication with another device over the Internet.

Mithyantha discloses these limitations. Ex. 3 ¶ 379.

8.1.12. SNQ IIa (§ 102)/Claims 25-26

25. The method according to claim 1, further comprising periodically sending, by the client device, a message that comprises a status of the client device, or is in response to the status of the client device.

26. The method according to claim 25, wherein the status is associated with being in the first or second state, and wherein the message is sent over the Internet to the first server.

As discussed in Section 8.1, Mithyantha discloses periodic or continuous determining of resource utilization, and shifting of states.

Further, when upstream router 700 refreshes its routing table at a predetermined time interval, if “client device” appliance/device 200’ is in the first state (*i.e.*, in response to the status of appliance/device 200’), appliance/device 200’ sends a message, via “first server” appliance/device 200, to upstream router 700 re-advertising its path.

“In some embodiments, after a predetermined period of time during which the upstream router 700’s routing table may expire and be refreshed, the active vServers 702a-702c, 702n may re-advertise their routes

with routing metric values restored or increased to their original values 706a-c, 706n.” Ex. 10 at 57:47-52, 57:52-61, 58:47-61, Fig. 7C.

Mithyantha discloses these limitations. Ex. 3 ¶ 383.

8.1.13. SNQ IIa (§ 102)/Claim 29

29. The method according to claim 1, wherein the web server uses HyperText Transfer Protocol (HTTP) and responds to HTTP requests via the Internet, and wherein the sending of the first content identifier to the web server comprises a HTTP request, or wherein the communication with the web server is based on, or uses, HTTP persistent connection, and wherein the first content includes, consists of, or comprises, a part or whole of files, text, numbers, audio, voice, multimedia, video, images, music, or computer program, or wherein the first content includes, consists of, or comprises, a part of, or a whole of, a web-site page.

As discussed in Section 8.1, Mithyantha discloses client(s) 102 that communicate with “one or more servers 106a-106n,” for example, when a web browser on a client 102 sends a request for a web page to a web server 106. Ex. 10 at 4:58-64, 6:52-53, 10:45-51, 11:1-24, 50-52, 23:55-58. Server 106 can be a web or HTTP server serving web pages in response to HTTP requests. *Id.* at 6:25-26, 6:52-53, 9:15-17, 11:13-17, 21:21-38, 21:57-64, 24:9-14, 27:43-45; see also *id.* at 10:54-67 (video and/or audio), 21:21-38 (voice (VoIP)), 32:10-29 (files and/or computer program).

Mithyantha discloses this limitation. Ex. 3 ¶ 385.

8.2. SNQ IIb (§ 103)/Obviousness of claims 1-2, 4-12, 15-26, and 28-29 over Mithyantha in View of Internet Standards, Standard Practices for Application Startup Configuration, and General Knowledge of a POSITA

If any Challenged Claim discussed in Section 8.1 is not anticipated by Mithyantha, the claim would have been obvious to a POSITA.

SNQ IIb combines the teaching of Mithyantha with the general knowledge of a POSITA with regard to HTTP and TCP/IP Internet communications, and resource utilization on general computers.

Mithyantha could also be combined with the disclosure of RFC 2616 itself as discussed herein.

The '614 patent assumes a basic understanding of computers and Internet communications, including HTTP and TCP/IP. The '614 patent discloses that data servers may be "HTTP servers, sometimes known as web servers." Ex. 1 at 31:57-59. The '614 patent defines the Internet in terms of "use [of] the standardized Internet Protocol Suite (TCP/IP)." *Id.* at 1:31-33.

The '614 patent cites RFC 2616 (and other RFCs) for a definition of HTTP, *id.* at 4:67-5:7, and cites RFC 2616 as prior art, *id.* at 3.

A POSITA would possess the types of knowledge referenced by the '614 patent, and as of 2013 would have been knowledgeable concerning the pertinent Internet protocols. Ex. 3 ¶ 391.

A POSITA would have been motivated to combine the disclosure of Mithyantha with a POSITA's general Internet knowledge (as noted in the claim-by-claim application below) and/or the disclosures of RFC 2616 governing the HTTP protocol. As explained in Section 8.1 regarding anticipation, Mithyantha concerns Internet communications and standard protocols HTTP, HTML, URLs, and TCP/IP.

A POSITA would understand that Mithyantha, and the '614 patent, call upon a POSITA to make reference to such background knowledge, and a POSITA would do so. Ex. 3 ¶ 393.

8.2.1. SNQ IIb (§ 103 + Internet Standards, Standard Practices for Application Startup Configuration, and General Knowledge of a POSITA)/Claim 1

As to “initiating, by the client device, communication” that comprises sending “the first identifier,” this limitation would have been obvious based on Mithyantha combined with the general knowledge of a POSITA and RFC 2616.

It is also explicit in the '614 patent that any device “which accesses a server over the Internet for a service or a resource” may be regarded as a client device. Ex. 1 at 4:53-57. On that basis, appliance/device 200' of Mithyantha clearly qualifies as a “client device” based on its accessing of servers 106a-106n for content. In any case it would have been obvious, in view of RFC 2616, that insofar as appliance/device 200' of Mithyantha is acting as a proxy for retrieving web content for clients 102a-102n, appliance/device 200' acts as both a client and a server. Ex. 12 at 10.

Mithyantha discloses that “client device” appliance/device 200' and “first server” appliance/device 200 communicate over Internet networks 104' and 104 using “any TCP/IP based protocol,” including HTTP. Ex. 10 at 5:3-7, 19:4-8, 21:21-38, 28:55-58, Fig. 1B. It would have been obvious to a POSITA based on his/her knowledge of Internet communications, TCP/IP, and HTTP (including the relevant RFC standards) that any communicating device in Mithyantha could initiate communications with the other by sending a communication (upon connection to the Internet) with the IP address or identifier of the device. Ex. 3 ¶ 396.

To any extent that it is not already necessarily implicit in Mithyantha appliance/device 200' sends its IP address to appliance/device 200 (the first server), this would have been obvious to a POSITA, in that Mithyantha expressly discloses that the IP address is sent to upstream router 700 *through* appliance/device 200, that the IP address thereby also goes to appliance/device 200, which relays it to upstream router 700. This is particularly clear, in view of the described embodiments in which each appliance/device 200 runs (*i.e.*, has within it) vServer 702, which specifically has the capability for “receiving, intercepting, processing, and/or forwarding packets to and from nodes of the cluster, servers, clients, or any combination of devices.” See Ex. 10 at 56:17-36. It is therefore obvious if not implicit that in the routing illustrated in Mithyantha, the IP address of appliance/device 200 goes (or would go) from appliance/device 200' to appliance/device 200.

To the extent it may not be necessarily implicit in Mithyantha's disclosure for the appliance/device 200' to initiate its communication with the first server “in response to connecting to the Internet,” it would have been obvious to do so. The stated purpose of appliance/device 200 is optimizing network services for the other devices in the network (Ex. 10 at 8:4-24). A POSITA would have been motivated to maximize this improvement by using well-known methods to incorporate this functionality upon startup of the respective devices, in order to make the improved capability provided by Mithyantha available immediately and automatically for all of the users' communications. Ex. 3 ¶ 398. The implementation for starting a program or service upon system initialization or bootup of a system was well known and routine as of 2013, as reflected in standard operating system documentation, for example the Windows manuals in Exs. 24, 25,

and 26 for setting programs that run on startup or installing programs to run in the background as a service. Following those prescriptions for setting up applications and services on device startup would have been an obvious exercise for any POSITA, with predictable results.

Mithyantha discloses a system comprised of typical computers and operating systems that include, for example, “any of the versions of Microsoft Windows.” *Id.* at 13:65-14:14, 16:27-45. A POSITA would also have been aware that Windows provides for assessment of resource utilization in standard computers using Windows Task Manager or Windows Resource Monitor. *See* Exs. 24, 25, and 26; Ex. 3 ¶ 399.

It would have been obvious that the devices disclosed in Mithyantha also could have used such native Windows functionality to assess resource utilization, including, for example, CPU, memory, or bandwidth utilization, as part of its determination of resource utilization. Ex. 3 ¶ 400.

As to “staying” or “shifting” between a first and second state, these limitations would have been obvious based on Mithyantha combined with a POSITA’s knowledge concerning general computers. Mithyantha discloses that appliance/device 200’ could determine itself to be in an “available” state in one scenario, and an “unavailable” state in another. Capturing this determination in a variable that continues to reflect this determination would have been an obvious programming choice, in that it lets the device itself determine when to determine its state, potentially unnecessary/excessive *ad hoc* interruptions to determine availability and allowing the device itself to determine the best test for its own availability, independent of the device to which it is responding. This rationale is reflected in the well-known design pattern known as the “State” pattern, as documented in the 1995 “Gang of Four” reference work on Design Patterns, widely read

by those of skill in the field as of 2013. Ex. 27 at 305-13 (describing the “State” Design Pattern, a “behavioral” software design pattern that allows an object to alter its behavior when its internal state changes); Ex. 3 ¶ 401.

As to “first content identifier,” this limitation would have been obvious based on Mithyantha combined with the general knowledge of a POSITA and RFC 2616. Mithyantha discloses the use of HTTP and requests sent from a web browser to a web server. Ex. 10 at 4:58-64, 6:52-53, 10:45-51, 11:1-24, 11:50-52, 23:55-58.

A POSITA would have understood that HTTP requests involved content identifiers for web content, typically a URL. RFC 2616, which concerns HTTP 1.1, discloses “GET” requests, which include URLs, *i.e.*, content identifiers. Ex. 12 at 35. The HTTP request includes the content identifier (*e.g.*, URL) so that the web content may be identified on the web server and returned to client 102. Facilitating such transactions is a primary point of Mithyantha. In the context of a claim that already expressly recites “fetching . . . a first content . . . from a web server,” it would have been obvious to a POSITA (if not indeed necessary) to include a content identifier (*e.g.*, URL) in passing a content request to the Web browser. Ex. 3 ¶ 403.

Similarly, again to such extent as may not otherwise have been completely implicit, it would have been obvious to any POSITA familiar with a web browser that the HTTP web browser requests disclosed in Mithyantha, *see e.g.*, Ex. 10 at 10:45-61, 11:50-52, 23:57-58, would cause a web server to respond with first content (*e.g.*, a web page) to be delivered to the web browser where the HTTP request originated. Ex. 3 ¶ 404.

Indeed, all of the claim 1 “back end” steps [1.7]-[1.11] are completely obvious as steps to retrieve web content, because they reflect no more than ordinary, run-of-the-mill proxied web content retrieval, as well docu-

mented for decades in standards such as Ex. 12 at 35, and books such as Ex. 13.

Mithyantha combines the two major aspects of claim 1: the state monitoring of the agent devices, and the proxied retrieval of web content through those agent devices. Thus claim 1, to the extent it might not be considered expressly or inherently anticipated by Mithyantha, would have been obvious to a POSITA based on the express disclosures of Mithyantha and the general knowledge of a POSITA as to Internet communications and general computing processes, as outlined above. Ex. 3 ¶ 406.

8.2.2. SNQ Iib (§ 103 + Internet Standards, Standard Practices for Application Startup Configuration, and General Knowledge of a POSITA)/Claim 2

2. The method according to claim 1, wherein the determining is performed by the client device.

This limitation would have been obvious based on Mithyantha combined with a POSITA's knowledge concerning general computers, including concerning the assessment of resource utilization in standard computers using Windows Task Manager or Windows Resource Monitor. Mithyantha discloses a system comprised of typical computers serving as the "client device" appliance/device 200'. Ex. 10 at 13:65-14:14. Mithyantha further discloses use of "any of the versions of Microsoft Windows." *Id.* at 16:27-45. It would have been obvious that appliance/device 200' could assess resource utilization, including, for example, CPU, memory, or bandwidth utilization. Ex. 3 ¶ 407.

Claim 2 would have been obvious to a POSITA. Ex. 3 ¶ 408.

8.2.3. SNQ IIb (§ 103 + Internet Standards, Standard Practices for Application Startup Configuration, and General Knowledge of a POSITA)/Claim 5

5. The method according to claim 4, further comprising establishing a connection with the first server, and wherein the communication with the first server is over the established connection, and wherein the communicating by the client device with the first server uses TCP, and wherein the connection is established by performing 'Active OPEN' or 'Passive OPEN'.

This limitation would have been obvious based on Mithyantha combined with the general knowledge of a POSITA and RFC 2616, including knowledge of Ex. 28 RFC 793 (TCP specification). Mithyantha discloses that appliance/device 200' may communicate with the first server using TCP. Section 8.1.3. For the same reasons, Claim 5 would have been obvious to a POSITA in view of the disclosure of RFC 793, which similarly reflects TCP communication details, such as Active and Passive open, with which a POSITA would have been familiar. See Section 8.1.4; Ex. 28 § 2.7, Fig. 6; Ex. 3 ¶ 409.

Claim 5 would have been obvious to a POSITA. *Id.* at ¶¶ 194-96.

8.2.4. SNQ IIb (§ 103 + Internet Standards, Standard Practices for Application Startup Configuration, and General Knowledge of a POSITA)/Claims 18-24

18. The method according to claim 1, wherein the resource comprises, or consists of, a hardware component in the client device.

19. The method according to claim 18, wherein the hardware component comprises, or consists of, a processor or Central Processing Unit (CPU) operation in the client device.

20. The method according to claim 19, wherein the resource utilization is based on, or comprises, the processor or CPU time of executing one or more threads or processes, wherein the resource utilization is based on, or comprises, the processor or CPU idling time, or wherein the resource utilization is based on, or comprises, the processor or CPU executing a system idle process.

21. The method according to claim 18, wherein the hardware component comprises, or consists of, a memory in the client device, and wherein the resource utilization is based on, or comprises, an amount of used or unused location or space of the memory.

22. The method according to claim 1, wherein the resource comprises, or consists of, input or output capability.

23. The method according to claim 22, wherein the resource comprises, or consists of, communication bandwidth of communication with another device over the Internet.

24. The method according to claim 23, wherein the resource comprises, or consists of, communication bandwidth of communication with the first server over the Internet, or wherein the resource utilization is based on, or according to, IETF RFC 2914.

Claims 18-24 concern resources related to the utilization of hardware (claim 18), such as a CPU (claims 19-20), memory (claim 21), I/O capability (claim 22), or bandwidth (claims 23-24).

These limitations would have been obvious based on Mithyantha combined with a POSITA's knowledge concerning general computers, including concerning the assessment of resource utilization in standard computers using Windows Task Manager or Windows Resource Monitor. Mithyantha discloses a system comprised of typical computers serving as "client device" appliance/device 200'. Ex. 10 at 13:65-14:14. Mithyantha further discloses extensive hardware included in that device. *Id.* at 14:3-16:17.

A CPU is explicitly disclosed, *id.* at 14:5-7, 14:15-27, as is "monitoring CPU utilization rate past a threshold for a predetermined time," *id.* at 56:61-57:14. A POSITA would have been motivated to use appliance/device 200' to assess hardware resource utilization, operation, execution time, idle time, and/or idle processes, including the CPU functions in appliance/device 200, for the same resource utilization purpose. Ex. 3 ¶ 413.

Input or output capability is explicitly disclosed as part of the device, as is monitoring "bandwidth." *Id.* at 11:46-12:7, 12:5-7, 12:12-19, 12:45-49, 13:3-13, 13:42-44, 15:26-39, 16:18-26, 56:61-57:14, Fig. 1E, Fig. 1F. It would have been obvious that appliance/device 200' could assess resource utilization, including input/output and its own communication bandwidth utilization, as part of resource utilization. Ex. 3 ¶ 414.

Claims 18-24 would have been obvious to a POSITA. Ex. 3 ¶ 415.

8.2.5. SNQ IIb (§ 103 + Internet Standards, Standard Practices for Application Startup Configuration, and General Knowledge of a POSITA)/Claim 28

28. The method according to claim 1, further comprising sending, by the client device, a physical geographical location to the first server,

and wherein the physical geographical location corresponds to the actual physical geographical location of the client device.

Claim 28 concerns the client device sending its geographic location to the first server. This limitation would have been obvious based on the disclosure of Mithyantha combined with the general knowledge of a POSITA and RFC 2616, including knowledge of “IP-based geolocation (commonly known as geolocation)[,which] is a mapping of an IP address. . . to the real-world geographic location of a computing device or a mobile device connected to the Internet.” Ex. 1 at 128:27-30, 93:22-30, 128:27-129:28, 129:46-54. The ’614 patent broadly defines geolocation and the determination of location based on IP addresses, and cites extensively to prior art that evidences that IP-based geolocation well-known long before 2013. *Id.* at 93:22-30, 128:27-129:28, 129:46-54; Ex. 3 ¶ 416; Ex. 33 at 3 (“Common sources of location information include . . . location inferred from network signals such as IP address”); Ex. 34 (disclosing methods for geolocating IP addresses).

Further, as discussed with regard to anticipation, Mithyantha discloses that “client device” appliance/device 200’ sends a first identifier (the IP address associated with the appliance/device 200’) to “first server” appliance/device 200 over the Internet. Further, Mithyantha teaches that one of the roles of upstream router 700 is to understand the various routing paths within the system and, based on metrics about those paths, or the availability/unavailability of certain devices along each path, distribute traffic to the more desirable paths. Ex. 10 at 56:37-60, 57:11-21. Mithyantha discloses that such metrics can include “local preference, . . . AS-path length, . . . origin type, origin, . . . or any other type and form of metric[, and m]ultiple metrics may be advertised so that the upstream

router 700 may apply different routing protocols to determine the next hop for packets[, and] metrics may represent . . . length, or any other values.” Ex 1011 at 56:37-42. Further, Mithyantha discloses that appliances 200’ may be geographically distributed and “load balancing may be weighted by location, or similar steps can be taken to mitigate any latency.” *Id.* at 52:51-53:4.

In order to distribute traffic to more desirable paths, it would have been obvious to a POSITA to modify the disclosure of Mithyantha such that the appliance/device 200’ sends its actual physical geographical location to the appliance/device 200 along with its IP address so that upstream router 700 may consider the geographic location of appliance/device 200’ when selecting the most desirable path, in order to perform such load balancing based on location.

Alternatively, it would be obvious to a POSITA to incorporate well-known, prior art IP-based geolocation methods into the system of Mithyantha in order to allow the appliance/device 200 or upstream router 700 to determine the actual physical geographical location of appliance/device 200’ in order to select the most desirable path. Ex. 3 ¶ 419.

Claim 28 would have been obvious to a POSITA. Ex. 3 ¶ 420.

8.2.6. SNQ IIb (§ 103 + Internet Standards, Standard Practices for Application Startup Configuration, and General Knowledge of a POSITA)/Claims 4, 6-12, 15-17, 25-26, 29

As set forth above in Sections 8.1.3-8.1.13, Mithyantha discloses the additional limitations of claims 4, 6-12, 15-17, 25-26, and 29. Therefore, if Claim 1 is rendered obvious by Mithyantha in view of both the general

knowledge of a POSITA and the disclosure of RFC 2616, these claims are also rendered obvious. Ex. 3 ¶ 421.

9. SNQ III: OBVIOUSNESS OF CLAIMS 1-2, 4-5, 7-10, 13, 17-26, AND 29 OVER MORPHMIX IN VIEW OF STANDARD PRACTICES FOR APPLICATION STARTUP CONFIGURATION AND GENERAL KNOWLEDGE OF A POSITA

The '614 patent states that anonymous web browsing is one of its objects. Ex. 1, 87:66-67. To a similar end, MorphMix states its goal as “achieving anonymous Internet access,” which, like the '614 patent, it also does with a plurality of agent devices, *i.e.*, with “a large number of nodes distributed all around the world.” Ex. 11 at 14, 109. (Citations use the MorphMix pagination: page 1 (page 21 of Ex. 11) is the first page of the thesis.)

The following figure illustrates the idea behind MorphMix:

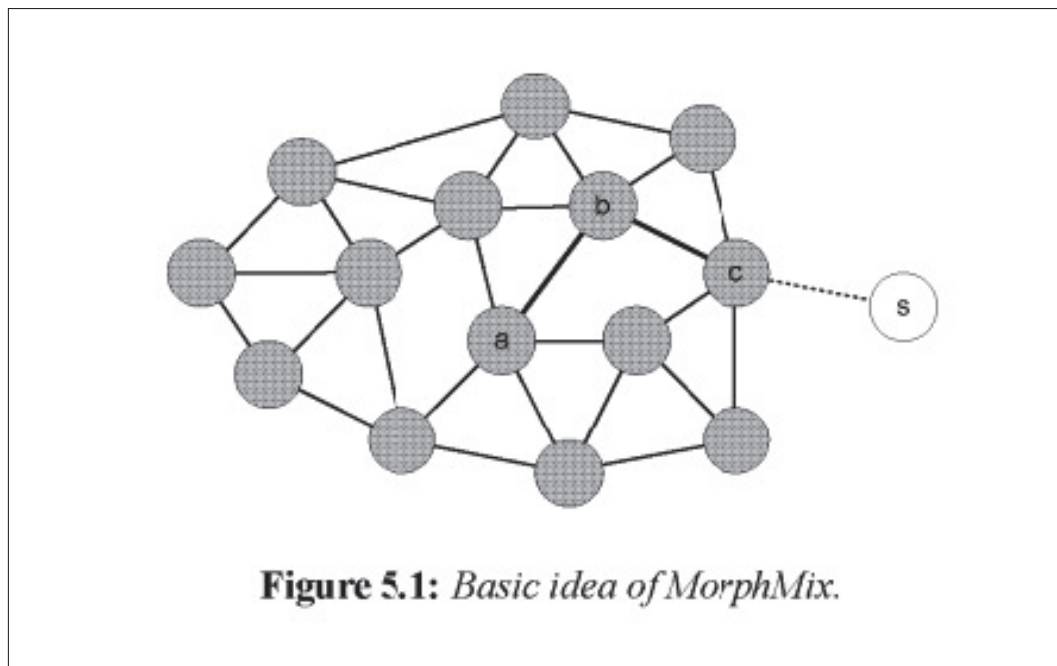


Figure 5 from MorphMix

Essentially, MorphMix hides a user a's identity from a web server (s) by not only interposing a proxy (c) between the user and the web server, but by further scrambling the route from the user to the web server over a "tunnel" of intermediate devices (including the last node/proxy), *e.g.*, by going through nodes b and c (though there may of course be additional nodes).

An individual can join MorphMix (and thereby also become such a "node") with a computer "connected to the Internet" that has an IP address and is capable of running applications "such as web browsers." *Id.* at 234.

MorphMix nodes are identified by their IP addresses and connect to other nodes with a TCP connection. *Id.* at 98-99. To access an Internet web server anonymously, a node "establishes a circuit via some other nodes" forming an "anonymous tunnel." *Id.* at 99. One example path of nodes is initiator (a) sending a request to intermediate node (b), which sends the request to the last node (c), which sends the request to server (s):

Id. at 98-100. (This example path will be used throughout the discussion that follows.)

When a web browser sends a request to a node, the first node sends the IP address and port of the targeted web server "to the final node." *Id.* at 103. The final node then "connects to the server" establishing an "end-to-end communication relationship." *Id.* "Sending data back from the server to the client works exactly in the opposite way." *Id.* at 105. *See also* Ex. 3 ¶ 428.

To the extent MorphMix fails to disclose any of the claimed details of the '614 patent, those are made obvious by the well-known considerations and techniques within the general knowledge of a POSITA.

9.1. SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA/Claim 1

[1.P] A method for use with a resource associated with a criterion in a client device that communicates with a first server over the Internet, the client device is identified in the Internet using a first identifier and is associated with first and second state according to a utilization of the resource, the method comprising:

Each preamble element is satisfied for the reasons provided in the discussion of claim steps [1.1]-[1.11], mapping onto MorphMix (in the discussed example path) as follows:

Client device: last node (c).

First server: intermediate node (b).

Resource: either (1) tunneling resources or (2) communication resources

Criterion: either (1) sufficient resources or insufficient resources or (2) sufficient CREDIT or insufficient CREDIT

First state: either (1) available for tunneling or (2) able to relay communications

Second state: either (1) not available for tunneling or (2) not able to relay communications

Briefly, with regard to the preamble,

A method for use with a resource associated with a criterion in a client device

During tunnel setup, the system checks the availability of nodes to participate in the tunnel, checking tunneling or communication resources against the criteria of sufficiency resources or of Credit (as further dis-

cussed below in connection with claim step [1.2]). See Ex. 11 at 98, 114, 116-18, 148, 199, 232, 272-73.

that communicates with a first server over the Internet

The nodes in MorphMix communicate over the Internet. The devices in the MorphMix “tunnel” are all clients (the all run web browsers and use the MorphMix system as well as participate as nodes in the system). Each device also acts as a server with respect to other devices in the tunnel. In the example give, device (b) may be regarded as the first server, and device c, which may be regarded as a client device, communicates with device (b), over the Internet.

the client device is identified in the Internet using a first identifier

The client device (node c) is identified in the Internet using a first identifier, which is its IP address.

and is associated with first and second state according to a utilization of the resource

As discussed in connection with step [1.2] below, MorphMix has “states” based on resource availability and “Credit.”

MorphMix discloses the preamble. Ex. 3 ¶ 436.

MorphMix etc. (§ 103) vs. Claim Step [1.1]—initiating, by the client device, communication with the first server over the Internet in response to connecting to the Internet, the communication comprises sending, by the client device, the first identifier to the first server over the Internet”

First, MorphMix discloses that the “client device” (node (c)) sends a “first identifier” (node (c)’s IP address) to the “first server” (node (b)) over the Internet.

Morphmix interconnects nodes “connected to the Internet.” Ex. 11 at 96. Every MorphMix node “can itself establish circuits via other nodes to access a server anonymously, but can also be part of circuits established by other nodes and relay data for them at the same time.” *Id.* at 98. MorphMix nodes must establish “neighbours”—nodes connected by “virtual links.” *Id.* at 98-99, 267-68. A virtual link can be created by node (c) “first establish[ing] a TCP connection with b using ipb and pmmb,” which are node (b)’s IP address and port. *Id.* at 267. Node (c) then sends a link request message (“Link_REQ”) that includes node (c)’s IP address and port. *Id.* Once node (b) accepts the connection and replies to node (c), the two nodes are “neighbours” via a virtual link and can commence with circuit-based communications. *Id.* at 98-99, 267-68.

“Nodes can join and leave the system at any time,” and “nodes may be shut down by their operators.” *Id.* at 98, 199. In the event of an operator shutdown, “the TCP connections from and to the computer will be correctly terminated [41], which tells the neighbours immediately that the connections and all tunnels using them are no longer usable.” *Id.* Upon reconnection to the Internet, the initial step of establishing “neighbour” status would then take place again. Both the initial set-up procedure and the restart scenario are examples of the “client device” initiating communication with the “first server.”

Second, MorphMix utilizes a “peer discovery mechanism that enables MorphMix nodes to learn about other nodes,” *id.* at 131, and “which allow a node to ask another MorphMix node for information about other nodes,

i.e. their IP addresses” and other information, *id.* at 132. “[A] node always includes its own node information when establishing a virtual link to another node . . . otherwise, a node could never inform other nodes about itself and consequently, no other node would establish a virtual link to it.” *Id.* at 133. Thus, MorphMix discloses that a node (*e.g.*, node (c)), when joining MorphMix, sends its node information to other nodes (*e.g.*, node (b)), including its IP address.

Communications between nodes (including for example a communication from node (c) to node (b)) use HTTP and TCP communications. *Id.* at 102-03 (“MorphMix can “anonymise [sic] any TCP-based application” and focuses on HTTP(S) web browsing). A POSITA would understand, that devices communicating over the Internet would send an identifier to facilitate communication.

A MorphMix node simply must have an IP address and port number. *Id.* at 98 (node is “identified with its public IP address”), 149 (MorphMix “can handle as many nodes as there are public IP addresses”). MorphMix discloses, for example, running MorphMix on both typical computer software, such as Linux (kernel 2.4.17), and on “Linux-VServer” software capable of operating multiple nodes on a single computer. *Id.* at 109, 129. As such, “node (b)” may be a “server” and “node (c)” may be a “client device.” *See, e.g.* Ex. 3 ¶ 442.

Since MorphMix is provided as a protective mechanism, to hide a user’s identity over the Internet, a POSITA would understand that tunnel setup and reconnection are steps that would be performed as early as possible, *i.e.*, “in response to connecting to the Internet.”

A POSITA, recognizing that it would be desirable to establish the protection of MorphMix for a user as early as possible when the user became

exposed to the Internet by establishing an Internet connection, would have found it obvious to address this need by making the MorphMix application a program that loaded and ran on device startup, as taught, for example, in Ex. 26, concerning automatically executing “startup” applications upon starting the Windows operating system. This well-known, simple step would cause MorphMix to start upon connection to the Internet, along with all of its initialization processes, including neighbor discovery, as discussed above. Ex. 3 ¶ 444.

Thus, MorphMix discloses this limitation or at a minimum it is rendered obvious over MorphMix in view of a POSITA’s general knowledge about configuring applications as “startup applications” in a computer system.

[1.2] when connected to the Internet, periodically or continuously determining whether the resource utilization satisfies the criterion

First, a “determining” in accordance with this limitation takes place during an anonymous tunnel setup. Nodes are added to tunnels “hop-by-hop.” Ex. 11 at 116.

Tunnel setup involves, in relevant part, node (c) receiving a tunnel setup message and “check[ing] if it is indeed willing to accept an anonymous tunnel from b.” *Id.* at 116-18 (step 6). If yes, node c responds OK and participates in building the tunnel. *Id.* (steps 6-10). However, “[i]f c does not accept being the next node in the tunnel or if there is another problem, c replies with a NEXT_FAIL message” *Id.* at 269. Node (c)’s willingness to serve in the anonymous tunnel depends in part on whether node (c) determines it has sufficient “spare resources” to support the tunnel. *Id.* at 114, 148, 232 (“A node can easily communicate with its neighbours to learn which of them are currently participating in MorphMix and have

spare resources to accept new anonymous tunnels.”). “Client device” node (c)’s determining whether it meets the criterion (having “spare resources”) discloses this limitation.

Node (c) performs this determining “periodically or continuously” because “anonymous tunnels are only used for a limited time”—specifically, ten minutes. *Id.* at 114. The ten-minute time limit, combined with MorphMix’s expectation that any node can utilize five tunnels at a given time, “results in setting up a tunnel every two minutes on average.” *Id.* Thus, in the example above, node (c) will be forced to “periodically or continuously” determine whether it has sufficient “spare resources” to support requested tunnels.

Second, a further “determining” that meets this limitation also takes place as a result of “flow control messages” that allow any node to avoid congestion by utilizing “a credit based scheme” that “works bidirectionally between two neighbouring nodes along an anonymous tunnel.” *Id.* at 272. For example, “node a gets an initial credit, which corresponds to the number of cells it is allowed to send to one specific neighbour b.” *Id.* at 273. “This initial credit is set to 50 cells, which means that a is allowed to send 50 cells belonging to this anonymous tunnel to b before it must wait.” *Id.* “Whenever b has forwarded 30 cells, it sends a CREDIT message back to a” which resets the credits “back to 50.” *Id.* But if b is unable to forward cells, it “stops sending back CREDIT messages,” and thereby “prevents a from sending cells” after “its credit is used up.” *Id.* at 273. In the exemplary node path discussed above, each of nodes (a), (b) (“first server”), and (c) (“client device”) employs this same credit-based flow control, “periodically or continuously” determining whether their resource utilization satisfies a criterion.

Both “determining” examples take place “when connected to the Internet,” as tunnel setup and flow control utilize messages sent from node to node, indicating activity taking place when connected to the Internet. *Id.* at 96 (goal of MorphMix is anonymous Internet access), 96 (Internet access required to join and use MorphMix), 98-100 (nodes communicate via IP addresses, ports, and TCP connections).

[1.3] responsive to the determining that the utilization of the resource satisfies the criterion, shifting to the first state or staying in the first state

The discussion of limitation [1.2] above provides two separate examples of a node (including “client device” node (c)) determining whether the utilization of the resource satisfies the criterion.

In the first example, node (c), based on the sufficiency of its resources to support a tunnel, will either accept or decline a tunnel setup request. If sufficient resources exist, the criterion will be determined satisfied and the tunnel setup will be accepted. Ex. 11 at 116-17, 269. This is shifting to or staying in the first state (available for tunneling). If not, the criterion will be determined not satisfied and the tunnel setup will be declined. *Id.* at 269; *see also id.* at 114, 148, 232. This is shifting to or staying in the second state (not available for tunneling).

In the second example, node (c) will either send a CREDIT message back to node (b), or it will not. *Id.* at 272-73. If the balance of cells warrants a CREDIT message, node (c) determines that the criterion is satisfied and sends a CREDIT message to node (b), thereby shifting to or staying in the first state (able to relay communications). *Id.* If the balance of cells does not warrant a CREDIT message, the criterion has not been satisfied and no

CREDIT message will be returned. *Id.* This will result in node (c) shifting to or staying in the second state (not able to relay communications).

MorphMix discloses this limitation. Ex. 3 ¶ 454.

[1.4] responsive to the determining that the utilization of the resource does not satisfy the criterion, shifting to the second state or staying in the second state

MorphMix's disclosures discussed directly above regarding claim step [1.3], incorporated here, satisfy this claim limitation.

MorphMix discloses this limitation. Ex. 3 ¶ 456.

[1.5] responsive to being in the first state, receiving, by the client device, a request from the first server

Node (c), when in the first state (available for tunneling and/or able to relay communications), can receive requests from node (b). Ex. 11 at 103-05, Fig. 5.4.

Such requests may include web browsing HTTP requests from initiator node (a) to server (s), sent using "an anonymous tunnel from a via b to c." *Id.* Step 9 of MorphMix's communication path description explains that node (b) forwards the HTTP request to node (c), and steps 10-12 explain how node (c) receives and processes that request. *Id.* at 105.

MorphMix discloses this limitation. Ex. 3 ¶ 459.

[1.6] performing a task, by the client device, in response to the receiving of the request from the first server

MorphMix's disclosures discussed directly above regarding claim step [1.5], incorporated here, satisfy this claim limitation. The "task" performed is further described below regarding claim steps [1.7]-[1.11].

MorphMix discloses this limitation. Ex. 3 ¶ 461.

[1.7] wherein the method is further configured for fetching over the Internet a first content identified by a first content identifier from a web server that is distinct from the first server, and the task comprising

MorphMix discloses a system to anonymously fetch content from a web server over the Internet. *See, e.g.*, Ex. 11 at 96 (goal of MorphMix is anonymous Internet access), 103 (focusing on “web browsing” and supporting HTTP(S)). An HTTP requests for web content are made from a client application (e.g., a web browser), which sends the request to node (a) in our ongoing example. *Id.* at 104. That HTTP request is then sent to a first server (node (b)) that then directs the request to a client device (node (c)). *Id.* at 104-05. The client device (node (c)) then forwards the HTTP request to web server (s). *Id.* The sought-after first content (e.g., a webpage) is returned via the same path: “Sending data back from the server to the client works exactly in the opposite way.” *Id.* at 105.

The “first content,” “first content identifier,” and steps that “comprise” this claim element are discussed below.

MorphMix discloses this limitation. Ex. 3 ¶ 464.

[1.8] receiving, by the client device, the first content identifier from the first server

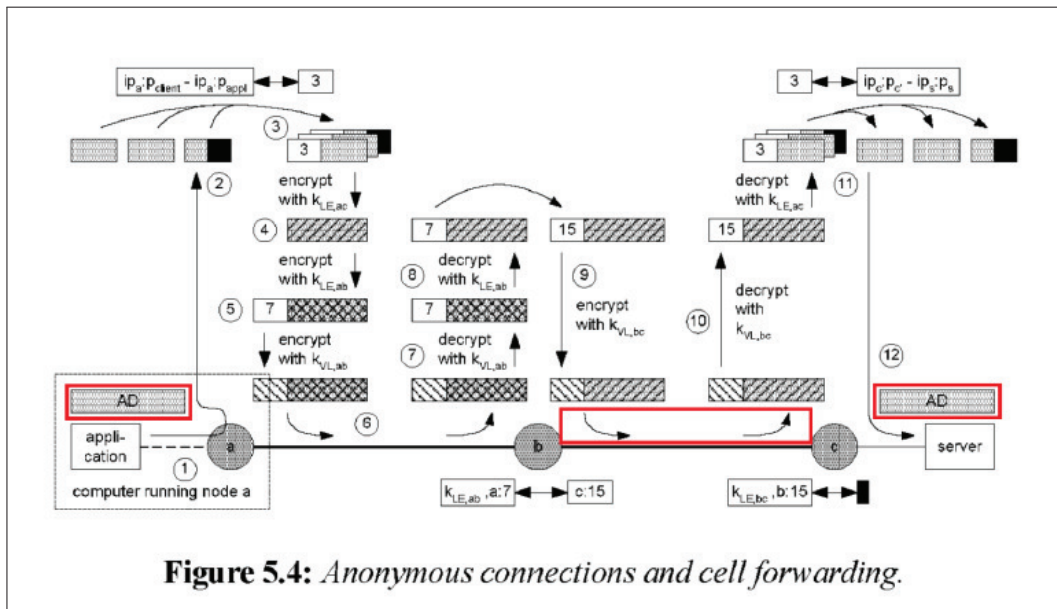
As explained directly above regarding claim step [1.7], incorporated here, node (c) acts as a proxy, enabling nodes (a) and (b) to connect to server (s): Ex. 11 at 98. The “first server” (node (b)), forwards the “first content identifier” (in the payload application data) to the “client device” (the final node (c)). *Id.* at 104-05.

The “application data” sent to the web server includes the data identifying the requested web page. MorphMix is focused on “web browsing,”

which involves the sending of HTTP requests. *Id.* at 103. “[I]n the case of web browsing, embedded objects in a web page are automatically re-requested by the browser.” *Id.* at 107.

MorphMix discloses that HTTP referrer headers, part of HTTP requests, include “the URL of the page the user is downloading.” *Id.* at 3-4. The ‘614 patent acknowledges that HTTP utilizes content identifiers, including URLs. Ex. 1 5:38-41. A POSITA would understand that the “application data” in MorphMix includes an HTTP request that includes a content identifier (*e.g.*, URL) identifying the target web page and related content. Ex. 3 ¶ 467.

Annotated Figure 5.4 shows this:



MorphMix, Fig. 5.4 (Annotated)

“[S]ending a web request as an initiator means that all other nodes along the anonymous tunnel must send and receive this request, too.” Ex. 11 at 218. Thus, application data (AD) within the payload is received by

“client device” node (c) (bottom right) from “first server” node (b) (bottom center). *Id.* at Fig. 5.4, 103-05 (step 9).

As discussed above in connection with limitation [1.1], MorphMix discloses that “a node” simply must have an IP address and port number, such that node (b) may be a “server” and node (c) may be a “client device.” Ex. 3 ¶ 470.

MorphMix discloses this limitation. Ex. 3 ¶ 471.

[1.9] sending, by the client device, the first content identifier to the web server

After the client device receives the first content identifier, the client device (node (c)), serving as proxy, sends the application data (AD) (which contains the first content identifier, e.g., URL) to the web server (server (s)). Ex. 11 at 103-105 (specifically, steps 11-12), Fig. 5.4. “[T]he connection between c and the server application is identified with the socket pair ipc:ipc’-ips:ps, which tells c to forward the data it receives . . .” *Id.* at 104. Again, a POSITA would understand that the “application data” includes a web page content identifier (e.g., URL). Ex. 3 ¶ 472.

MorphMix discloses this limitation. *Id.* at ¶¶ 251-52.

[1.10] receiving, by the client device, the first content from the web server in response to the sending of the first content identifier

After the “client device” node (c) sends the first content identifier (e.g., URL) to web server (s), node (c) receives, in response and still serving as proxy, the first content (e.g., web page content) from web server (s). Ex. 11 at 103-05 (step 12) (“Sending data back from the server to the client works exactly in the opposite way.”). Because the final node (c) is the only node connected to the web server, the web server’s response with first content

must be received by the client device. *Id.* at 100 (one TCP connection between final node and web server), Fig. 5.1, Fig. 5.4; *see also* MorphMix at 204 (the “web server” sends “a web reply after having completely received a web request”), 218 (“[T]he reply sent back by the web server must be sent and received by the final and all intermediate nodes along the tunnel.”).

The '614 patent acknowledges that “[a]n information resource is identified by a Uniform Resource Identifier (URI/URL) and may be part of a web page” and “the primary purpose of a web browser is to bring information resources to the user.” Ex. 1 at 20:4-27, 63:26-29 (“the first content may be a web-site, a web-page, or a URL”). A POSITA would understand that MorphMix’s HTTP web browser requests, Ex. 11 at 100, 103, 107, would cause a web server to respond with web page content to be delivered to the originating web browser. Ex. 3 ¶ 475.

MorphMix discloses this limitation. *Id.* at ¶¶ 253-255.

[1.11] sending, by the client device, the received first content to the first server

After the client device receives the first content (e.g., web page), “client device” node (c), serving as proxy, sends that content to “first server” node (b), which provides the first content (e.g., web page) up the same path to the requesting web browser. Ex. 11 at 103-05 (step 12) (“Sending data back from the server to the client works exactly in the opposite way.”), 218 (“[T]he reply sent back by the web server must be sent and received by the final and all intermediate nodes along the tunnel.”), Fig. 5.1, Fig. 5.4. Simulations analyzing web browsing specifically looked at “the time it takes to completely download a web page, which is defined as the time between sending the first byte of the web request for the index file and receiving the last byte of the complete page.” *Id.* at 205. A POSITA would

understand that MorphMix's HTTP web browser requests, Ex. 11 at 100, 103, 107, would cause a web server to respond with first content (*e.g.*, web page) to be delivered to the originating web browser. Ex. 3 ¶ 477.

MorphMix discloses this limitation. Ex. 3 ¶ 478.

9.2. SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claim 2

2. The method according to claim 1, wherein the determining is performed by the client device.

The discussion above concerning limitation [1.2] discusses two “determining” examples: tunnel setup and flow control.

Regarding tunnel setup, it is “client device” node (c) that receives a tunnel setup message, “checks if it is indeed willing to accept an anonymous tunnel from b,” and either responds OK or declines the request, for example, because of insufficient “spare resources.” Ex. 11 at 118, 148. “Client device” node (c) therefore determines whether it meets the criterion (whether it has sufficient “spare resources” to support the tunnel).

Regarding flow control, every node (including node (c)) uses flow control messaging to avoid congestion. *Id.* Thus, “client device” node (c) uses the “credit based scheme” for flow control and determines whether it is able to forward messages (and send CREDIT messages).

MorphMix discloses this limitation. Ex. 3 ¶ 482.

9.3. SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claim 4

4. The method according to claim 1, wherein the communication by the client device with the first server is based on, or is according to, TCP/IP protocol or connection.

“Client device” node (c) communicates with the “first server” node (b) via the TCP protocol or a TCP connection. Ex. 11 at 98 (“To be contacted by other nodes, a node listens on TCP port pmmi . . .”). The discussion above regarding limitation [1.1] discusses how node (c) establishes a virtual link with node (b). Node (c), for example, can “establish a TCP connection with b using ipb and pmmb,” node (b)’s IP address and port. *Id.*

MorphMix discloses this limitation. Ex. 3 ¶ 484.

9.4. SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claim 5

5. The method according to claim 4, further comprising establishing a connection with the first server, and wherein the communication with the first server is over the established connection, and wherein the communicating by the client device with the first server uses TCP, and wherein the connection is established by performing ‘Active OPEN’ or ‘Passive OPEN’.

The ‘614 patent acknowledges that “Active OPEN” and “Passive OPEN” are standard TCP establishment approaches. Ex. 1 at 2:41-65; Ex. 28 § 2.7. A POSITA would understand that the disclosure of TCP/IP, as described directly above, necessarily discloses these standard means of con-

necting. Ex. 3 ¶ 485. MorphMix cites the applicable standard, RFC 793. Ex. 11 at 249 n.41.

MorphMix discloses this limitation. Ex. 3 ¶ 486.

9.5. SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claim 7

7. The method according to claim 1, wherein the steps are sequentially executed.

MorphMix discloses the sequential execution of claim 1's steps. In the example described above, node (c) must send its identifier to node (b) in order to establish a virtual link. *See* Section 8.1.1. Node (b) can request that node (c) be added to an anonymous tunnel. *Id.* As part of such requests, node (c) will periodically or continuously determine whether its resource utilization can support a tunnel. *Id.* If node (c) first deems itself incapable of supporting a tunnel, but thereafter capable of supporting a tunnel for a second request, there will be a shift from first state, to second state, and back to first state. *Id.* Node (c) may thereafter receive a request from the first server, and thereafter perform the tasks, in sequential order, to fetch content. *Id.*

MorphMix discloses this limitation. Ex. 3 ¶ 488.

9.6. SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claim 8

8. The method according to claim 1, wherein the first identifier comprises an IP address that is in IPv4 or IPv6 form.

As discussed with regard to limitation [1.2], MorphMix discloses that the “client device” node (c) sends a “first identifier” (node (c)’s IP address) to the “first server” node (b) over the Internet. MorphMix “focuses on IP version 4 (IPv4)” and “heavily depends on the IPv4 addressing structure.” *Id.* at 144.

MorphMix also discloses a “first identifier” in IPv6 form. *Id.* at 144-47.

MorphMix discloses this limitation. Ex. 3 ¶ 491.

9.7. SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claims 9-10

9. The method according to claim 1, wherein the client device is further storing, operating, or using, a client operating system.

10. The method according to claim 9, wherein the client operating system consists or, comprises of, or is based on, one out of Microsoft Windows 7, Microsoft Windows XP, Microsoft Windows 8, Microsoft Windows 8.1, Linux, and Google Chrome OS.

“[A]ny state-of-the-art personal computer,” including those with modest bandwidth, “can run a MorphMix node.” Ex. 11 at 142. MorphMix acknowledges that an attack could manipulate “the operating system.” *Id.* at 152. MorphMix discloses tests of its system on a typical computer “running Linux as operating system.” *Id.* at 129. A POSITA would understand that ordinary computers, such as used in MorphMix, would use an operating system. Ex. 3 ¶ 492.

MorphMix discloses these limitations. Ex. 3 ¶ 493.

9.8. SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claim 13

13. The method according to claim 1, further comprising executing an application, and wherein the application comprises a web browser.

As discussed in the introduction to Section 9, MorphMix discloses a web browser application that initiates an HTTP request for web content from a web server. Ex. 11 at 96, 100 (“Three client applications C1-C3 (e.g., web browser windows) on the initiator’s computer . . .”).

MorphMix discloses this limitation. Ex. 3 ¶ 495.

9.9. SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claim 17

17. The method according to claim 1, for use with a set threshold value, and wherein the criterion is satisfied when the resource utilization is above or below the threshold.

As discussed in connection with limitations [1.1] and [1.2], MorphMix discloses two examples of “determining” that takes place. Both examples involve a set threshold value, wherein satisfaction of the criterion is triggered in relation to that threshold. In the example of tunneling, the threshold value relates to the “spare resources” present, or not present, on a potential node. See discussions of limitations [1.1] and [1.2].

MorphMix reported CPU “computational overhead of about 6%,” “easily” within their computer’s threshold. *Id.* In the example of flow control, the threshold value relates to a credit-based scheme (specifically, a threshold of 30 forwarded credits) tracked by each node, where the downstream

node sends (or declines to send) credits depending on whether it can forward messages. *Id.* at 272-73. Whether resource utilization is above or below each threshold determines whether each respective criterion has been satisfied.

MorphMix discloses this limitation. Ex. 3 ¶ 498.

9.10. SNQ III (§ 103 Morphmix + Standard Practices for Application Startup Configuration and General Knowledge of a POSITA)/Claims 18-24

18. The method according to claim 1, wherein the resource comprises, or consists of, a hardware component in the client device.

19. The method according to claim 18, wherein the hardware component comprises, or consists of, a processor or Central Processing Unit (CPU) operation in the client device.

20. The method according to claim 19, wherein the resource utilization is based on, or comprises, the processor or CPU time of executing one or more threads or processes, wherein the resource utilization is based on, or comprises, the processor or CPU idling time, or wherein the resource utilization is based on, or comprises, the processor or CPU executing a system idle process.

21. The method according to claim 18, wherein the hardware component comprises, or consists of, a memory in the client device, and wherein the resource utilization is based on, or comprises, an amount of used or unused location or space of the memory.

22. The method according to claim 1, wherein the resource comprises, or consists of, input or output capability.

23. The method according to claim 22, wherein the resource comprises, or consists of, communication bandwidth of communication with another device over the Internet.

24. The method according to claim 23, wherein the resource comprises, or consists of, communication bandwidth of communication with the first server over the Internet, or wherein the resource utilization is based on, or according to, IETF RFC 2914.

Claims 18-24 concern resources related to the utilization of hardware (claim 18), such as a CPU (claims 19-20), memory (claim 21), I/O capability (claim 22), or bandwidth (claims 23-24).

As discussed in connection with limitations [1.1] and [1.2], MorphMix discloses two examples of “determining” when utilization of a resource satisfies a criterion, which are (i) in connection with setting up tunneling, and (ii) in carrying out flow control.

In the context of setting up tunnels in MorphMix, a potential node must have “spare resources” capable of supporting a tunnel. See discussion above regarding limitations [1.1] and [1.2]. Examples of such resources include at least “the computational overhead.” Ex. 11 at 140-41. In one test, “a computer equipped with a 1GHz AMD Athlon CPU” had “a computational overhead of about 6%.” *Id.* at 221. Thus, in this example the resource comprises or consists of a hardware component in the client device: specifically, the CPU of node (c), which itself comprises CPU operation, including, for example, execution times, idling times, and idle processes, addressing claims 18, 19, and 20.

In the context of flow control, MorphMix discloses that each node determines whether its own utilization of communication resources is sufficient or insufficient to warrant issuance of CREDIT messages to prior nodes to allow more cells to be delivered. *See* discussion above regarding limitations [1.1] and [1.2]. This is done to avoid the node using up its memory, relevant to claim 21. The implementation in MorphMix uses “CREDITS” to represent how much more input a node can accept, and thus its available memory capacity. *See* Ex. 11 at 272; Ex. 3 ¶ 502. Thus, a node’s acceptance of content retrieval tasks is based on a determination of how much CREDIT it has, representing the extent of existing utilization of its memory. *Id.*

With regard to claims 22-24, MorphMix further discloses that “nodes that do not have the capabilities to relay many anonymous tunnels because of the bandwidth limitations . . . are offered less frequently in selections, reflecting a determination based on utilization of bandwidth and/or I/O capacity. *See* Ex. 11 at 183; Ex. 3 ¶ 503. To the extent this does not disclose affirmatively making a “determination” based on I/O or bandwidth utilization, it is clearly a suggestion to do so, based on the disclosure that the hardware in in any case causing selections based on I/O or bandwidth to take place. It would therefore have been obvious to take the further step to build in a further or alternate mechanism, in addition to or in lieu of the disclosed “CREDITS,” but based on a current measurement of I/O or bandwidth load on the node device, something easily determined using common tools such as the Windows task manager (Ex. 26) previously discussed, and like standalone utilities. *See* Ex. 3 ¶ 503.

MorphMix thus discloses the limitations of claims 18-21 and renders claims 22-24 obvious. Ex. 3 ¶ 504.

9.11. SNQ III (§ 103 Morphmix + Standard Practice for Application Startup Configuration and General Knowledge of a POSITA)/Claims 25-26

25. The method according to claim 1, further comprising periodically sending, by the client device, a message that comprises a status of the client device, or is in response to the status of the client device.

26. The method according to claim 25, wherein the status is associated with being in the first or second state, and wherein the message is sent over the Internet to the first server.

As discussed in Sections [1.1] and [1.2], MorphMix discloses two examples of periodically or continuously “determining” resource utilization, as well as shifting to and staying in first and second states.

For tunnel setup, if node (c) is “willing to accept an anonymous tunnel from b” node c responds OK and participates in key encryption exchanges to build the tunnel. See discussion of limitation [1.2]. As part of that key encryption exchange, “client device” node (c) sends its half of the encryption key-exchange to “first server” node (b). Ex. 11 at 116-18 (step 9). This processes periodically repeats itself as new tunnels are created (every two minutes on average). *Id.* at 114.

For flow control, in relevant part, “client device” node (c) will periodically send CREDIT messages back to “first server” node (b) largely dependent on the input/output hardware and related Internet connection of each node (affecting bandwidth, and thus, flow rates). See discussion above regarding limitation [1.2].

Both tunnel setup and flow control utilize messages sent from node to node, indicating messages being sent over the Internet. Ex. 11 at 96 (Internet access required to join and use MorphMix).

MorphMix discloses these limitations. Ex. 3 ¶ 509.

9.12. SNQ III (§ 103 Morphmix + Standard Practice for Application Startup Configuration and General Knowledge of a POSITA)/Claim 29

29. The method according to claim 1, wherein the web server uses HyperText Transfer Protocol (HTTP) and responds to HTTP requests via the Internet, and wherein the sending of the first content identifier to the web server comprises a HTTP request, or wherein the communication with the web server is based on, or uses, HTTP persistent connection, and wherein the first content includes, consists of, or comprises, a part or whole of files, text, numbers, audio, voice, multimedia, video, images, music, or computer program, or wherein the first content includes, consists of, or comprises, a part of, or a whole of, a web-site page.

MorphMix discloses a system that can be used to fetch content from a web server over the Internet. Ex. 11 at 103 (focusing on “web browsing” and supporting HTTP(S)). As explained above, server (s) can (1) be a web server, (2) receive requests for webpages made over HTTP, and (3) serve webpages in response to requests for the same. *Id.* at 103, 107, 168, 204, 205, 207, 215. Thus, server (s) uses HTTP, receives HTTP requests with first content identifiers (URLs), and serves content that consists of webpages. *See also id.* at 236 (regarding files).

MorphMix discloses this limitation. Ex. 3 ¶ 511.

10. CONCLUSION

Based on the foregoing, Requester respectfully requests reexamination of the Challenged Claims. Requester further requests that upon such re-examination, a certificate be issued cancelling the Challenged Claims as unpatentable.

/Ronald Abramson/
Ronald Abramson

Dated: October 9, 2021