

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

METACLUSTER LT, UAB,
Petitioner,

v.

BRIGHT DATA LTD.,
Patent Owner.

Case IPR2022-00687
Patent 11,190,622

DECLARATION OF JAMES OLIVIER, Ph.D

Metacluster LT, UAB

EX1002

Page 1 of 132

Ex.1029 / IPR2024-00503 / Page 1 of 132

CISCO SYSTEMS, INC. v. PORTSMOUTH NETWORK CORP.

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	PROFESSIONAL BACKGROUND.....	1
III.	COMPENSATION.....	5
IV.	OVERVIEW OF TASK & BASIS FOR OPINIONS	6
V.	LEGAL CONSIDERATIONS	7
VI.	LEVEL OF ORDINARY SKILL IN THE ART	10
VII.	OVERVIEW OF THE TECHNICAL FIELD & PRIOR ART	12
	A. RFC 2616	12
	B. RFC 791	15
	C. RFC 793	18
VIII.	CLAIM CONSTRUCTION	20
	A. “Client Device” and “First Server”	21
	B. “Selecting, in response to the receiving of the [first / second] URL”	22
	C. “First server” “sending ... to the [first / second] web server using the selected IP address”	23
	D. “... using the selected IP address as a source address”.....	23
IX.	THE ’622 PATENT	24
X.	OVERVIEW OF PRIOR ART REFERENCES.....	26
	A. U.S. Pat. No. 6,785,705 (“Kocherlakota”) EX1003	26
	B. RFC 1122	36
	C. U.S. Pat. No. 6,389,462 (“Cohen”).....	37
XI.	COMPARISON OF THE PRIOR ART TO THE CLAIMS.....	40
	A. Ground 1 – Kocherlakota Renders Obvious Claims 1-7, 10, 14, 16-17, 20-24, 26-32	41
	1. <i>Claim 1</i>	41
	2. <i>Claim 2</i>	54
	3. <i>Claim 3</i>	55
	4. <i>Claim 4</i>	55
	5. <i>Claim 5</i>	56
	6. <i>Claim 6</i>	57

7.	<i>Claim 7</i>	58
8.	<i>Claim 10</i>	58
9.	<i>Claim 14</i>	60
10.	<i>Claim 16</i>	60
11.	<i>Claim 17</i>	61
12.	<i>Claim 20</i>	62
13.	<i>Claim 21</i>	63
14.	<i>Claim 22</i>	63
15.	<i>Claim 23</i>	64
16.	<i>Claim 24</i>	64
17.	<i>Claim 26</i>	64
18.	<i>Claim 27</i>	65
19.	<i>Claim 28</i>	66
20.	<i>Claim 29</i>	67
21.	<i>Claim 30</i>	67
22.	<i>Claim 31</i>	68
23.	<i>Claim 32</i>	68
B.	Ground 2 – Kocherlakota in View of RFC 1122 Renders Obvious Claims 8-9, 11-13	69
1.	<i>Motivation to combine</i>	70
2.	<i>Modification of Kocherlakota in view of RFC 1122</i>	72
3.	<i>Claim 8</i>	73
4.	<i>Claim 9</i>	73
5.	<i>Claim 11</i>	73
6.	<i>Claim 12</i>	74
7.	<i>Claim 13</i>	74
C.	Ground 3 – Cohen Renders Obvious Claims 1-14, 17, 20-24, 26-32.....	75
1.	<i>Claim 1</i>	75
2.	<i>Claim 2</i>	85
3.	<i>Claim 3</i>	86

4.	<i>Claim 4</i>	86
5.	<i>Claim 5</i>	88
6.	<i>Claim 6</i>	89
7.	<i>Claim 7</i>	90
8.	<i>Claim 8</i>	90
9.	<i>Claim 9</i>	92
10.	<i>Claim 10</i>	92
11.	<i>Claim 11</i>	94
12.	<i>Claim 12</i>	95
13.	<i>Claim 13</i>	95
14.	<i>Claim 14</i>	95
15.	<i>Claim 17</i>	96
16.	<i>Claim 20</i>	96
17.	<i>Claim 21</i>	96
18.	<i>Claim 22</i>	96
19.	<i>Claim 23</i>	97
20.	<i>Claim 24</i>	98
21.	<i>Claim 26</i>	98
22.	<i>Claim 27</i>	99
23.	<i>Claim 28</i>	99
24.	<i>Claim 29</i>	100
25.	<i>Claim 30</i>	100
26.	<i>Claim 31</i>	101
27.	<i>Claim 32</i>	102
XII.	Conclusion	103

PETITIONER’S EXHIBIT LIST

Exhibit	Shorthand	Description
1001	'622 Patent	U.S. Patent No. 11,190,622
1002	Olivier	Declaration of Dr. James Olivier
1003	Kocherlakota	U.S. Patent No. 6,785,705 to Kocherlakota (Aug. 31, 2004) (“Kocherlakota”)
1004	Cohen	U.S. Patent No. 6,389,462 to Cohen (May 14, 2002) (“Cohen”)
1005	RFC 2616	Internet Engineering Task Force, <i>Hypertext Transfer Protocol – HTTP/1.1</i> , June 1999
1006	RFC 1122	Internet Engineering Task Force, <i>Requirements for Internet Hosts – Communication Layers</i> , October 1989
1007	'622 FH	Prosecution History of U.S. Patent No. 11,190,622
1008	'511 FH	Prosecution History of U.S. Patent No. 10,484,511
1009	'511 Reexam Decision	Order Granting Request for Ex Parte Reexamination of U.S. Patent No. 10,484,511 in 90/014,827
1010	<i>Teso</i> CC Order	Claim Construction Opinion and Order, Document 191, <i>Luminati Networks Ltd. v. Teso LT et al.</i> , Case No. 2:19-cv-00395 (E.D. Tex.)
1011	<i>Code200</i> CC Order	Claim Construction Memorandum Opinion and Order, Document 97, <i>Luminati Networks Ltd. v. Code200 et al.</i> , Case No. 2:19-cv-00396 (E.D. Tex.)
1012	Motion for Hearing	Defendants’ Motion for Hearing Regarding O2 Micro Issue, Document 444, <i>Bright Data Ltd. v. Teso LT et al.</i> , Case No. 2:19-cv-00395 (E.D. Tex.)
1013	Supplemental CC Order	Supplemental Claim Construction Order, Document 453, <i>Bright Data Ltd. v. Teso LT et al.</i> , Case No. 2:19-cv-00395 (E.D. Tex.)
1014	<i>Tefincom</i> '511 MSJ	Redacted Defendant’s Motion for Partial Summary Judgment of Noninfringement or in the Alternative Invalidity for the '511 Patent, Document 101, <i>Bright Data Ltd. v. Tefincom S.A. d/b/a NordVPN</i> , Case No. 2:19-cv-00414 (E.D. Tex.)

Exhibit	Shorthand	Description
1015	RFC 791	Internet Engineering Task Force, Request for Comments 1122 <i>Internet Protocol</i> , September 1981
1016	RFC 793	Internet Engineering Task Force, Request for Comments 1122 <i>Transmission Control Protocol</i> , September 1981
1017	RFC 1123	Internet Engineering Task Force, Request for Comments 1123 <i>Requirements for Internet Hosts - Application and Support</i> , October 1989
1018	Coley	U.S. Patent 5,826,014 to Coley (Oct. 20, 1998 (“Coley”))
1019	Haverstock	U.S. Patent No. 6,449,640 to Haverstock (Sep. 10, 2002) (“Haverstock”))

I. INTRODUCTION

1. My name is James L. Olivier, Ph.D. I have been retained by Metacluster Lt, Uab as an independent expert in the relevant art.

II. PROFESSIONAL BACKGROUND

2. I have a Ph.D. from The Ohio State University in Electrical Engineering with minors in Discrete Mathematics, Computer Science, and Microelectronics. I have published papers in the areas of coding theory and multiprocessor computer systems. I received my Bachelor of Science degree from Ohio State University in 1983. My CV is attached hereto as Appendix A, which shows my education and experience in more detail.

3. I have extensive experience in the design and development of telecommunication systems and have specialized experience in network product development.

4. I have developed and designed equipment for cellular networks since I first joined AT&T Bell Laboratories in 1990. From 1990 to 2005, I also designed and implemented a variety of telecommunication systems, including Asynchronous Transfer Mode (“ATM”) based systems for use in cellular networks. ATM is a broadband, packet-switched telecommunications standard defined by the American National Standards Institute (“ANSI”) and the International Telecommunication Union (“ITU”). I also participated in the design and development of AT&T

Autoplex Series base stations. I also participated in the design and development of AT&T's Network Control Points, 'NCPs' which were massive network databases containing subscription information for customers. During this time, I first began my work with telecommunication standards bodies as a contributing member of the ATM Forum.

5. In 1995, I transitioned to the Digital Switch Corporation ("DSC") Switch Products Division and was the Senior Manager of the ATM systems engineering group developing ATM packet switches for a new generation base station for use by Motorola in their Centralized Base Station Controller, a core part of the second generation cellular network. Later, as Senior Manager for Intelligent Networks, I designed and developed a video residential gateway, which was presented at SuperComm 1996.

6. I next worked at Samsung Telecommunications America from 1996 to 1999 as a Principal Engineer for Samsung's next generation wireless broadband switching system over the Universal Mobile Telecommunications System ("UMTS"). UMTS is a third-generation ("3G") broadband standard developed by the 3rd Generation Partnership Project ("3GPP"). My work at Samsung included designing their next generation UMTS cellular switch, which provided both packet and voice services, such as telephony services, wireless services, broadband services, and Internet services. While at Samsung, I also served as Samsung's North

American corporate representative to the ITU, which is the agency of the United Nations responsible for facilitating interconnectivity of information and communication technologies worldwide. The ITU participated in the 3GPP under the ITU's International Mobile Telecommunications 2000 effort. It was there that I participated in the development of standards for advanced wireless networks.

7. After that, I worked for Marconi Communications from 1999 to 2002, where I was responsible for design and development of a number of systems for the access market, including Digital Subscriber Line ("DSL") modems, along with the design of point-to-point wireless systems. I was also responsible for the servers for the Network Management System for the North American Access product division, which provide service provisioning for DSL customers. It was here where I architected a triple play residential gateway, which provided voice, video and data to residential subscribers.

8. I joined Navini Networks in 2002 as a Senior Manager. The Navini system was an entirely packet-based cellular system. I was responsible for layer 2 and layer 3 network protocols for Navini's Wideband Code Division Multiple Access ("WCDMA") wireless base stations and broadband modems. These layers were responsible for packet transmissions for various services over the WCDMA air interface. I also developed network-based servers and databases for network authentication, network services, service provisioning and subscriber management

for the Navini's Worldwide Interoperability for Microwave Access 'WiMAX' Network.

9. I have been the owner of Olivier Consulting since 2003 and have provided consulting services to various companies to develop networking systems and on intellectual property matters, including many such matters relating to networking technologies specifically.

10. I am currently Adjunct Executive in Residence in the Hunt Institute for Engineering and Humanity, which is part of the Lyle School of Engineering at Southern Methodist University in Dallas, Texas. Here, I serve as the Program Lead for Transformational Technology. As Program Lead, I am responsible for the Maps4Good project which uses SMU's data center servers to provide web-based services for the community, such as a COVID Relief Map.

11. I am also currently an Adjunct Professor in the Telecommunications and Network Engineering Program at Southern Methodist University's Graduate School of Electrical Engineering, where I teach classes in networking and networked enabled applications.

12. Overall, I have over 20 years of experience in advanced network engineering and product development. I have been recognized as an expert by the International Trade Commission ("ITC") in security and firewalls in routers and switches, cellphone hardware and software for imaging, operating systems for

mobile devices, mobile devices hardware and software architectures, and ethernet switch packet processor hardware and software.

13. I have also opined on the meaning of claim terms to one of ordinary skill in the art on numerous occasions. For example, I provided opinions on the meanings of claim terms in QPSX Developments 5 Pty Ltd. v. Nortel Networks, Inc and In the Matter of Certain Wireless Devices, Including Mobile Phone and Tablets II, USITC Inv. No. 337-TA-905.

14. My CV, which I understand is being submitted with this declaration, includes a listing of patents applications on which I am an inventor.

15. Because of my background, training, and experience, I am qualified as an expert to explain the background of the technology encompassed by the '622 Patent as well as to opine on the validity of the claims of the '622 Patent in view of the prior art references discussed herein.

16. If called upon to do so, I could and would testify truthfully regarding the points stated below in this declaration.

III. COMPENSATION

17. My work on this matter is being billed at my customary rate of 625.00 per hour. Also, I am being reimbursed for reasonable expenses I incur in relation to my services. I will be paid regardless of the outcome of any proceeding that my work is used in.

IV. OVERVIEW OF TASK & BASIS FOR OPINIONS

18. I have been asked to review the '622 Patent. I have been asked to provide opinions related to certain issues from the perspective of a person of ordinary skill, having knowledge of the relevant art, as of October 8, 2009, and—except where otherwise noted—the opinions stated in this declaration are from that perspective. The qualifications and abilities of such a person are described in paragraph 33 below.

19. More particularly, I have been informed that this proceeding is currently at a preliminary stage during which the Patent Trial and Appeal Board will decide whether the Petition establishes a reasonable likelihood of at least one claim of the '622 Patent being invalid.

20. My opinions are based on my education, training, and experience as well as items that I reviewed to prepare my opinions, including the documents listed in the Exhibit List included with the Petition and any other items I reference in my below analysis.

21. I understand that other issues may arise that require further explanation, and I will provide that explanation if appropriate. As a result, I respectfully reserve the right to update and supplement this declaration and the information and opinions provided herein.

V. LEGAL CONSIDERATIONS

22. I am not an attorney. My understanding of the law is based on information provided by counsel for Petitioner.

23. My opinions address what would have been logical to, and within the skill level of, a person of ordinary skill in the art (“POSITA”) at the time of the alleged invention, given the state of the relevant art, the knowledge and skill that a POSITA would have, the teachings of the references discussed below, and how a POSITA would have understood those teachings. My opinions also address whether a POSITA would have had a reasonable expectation of the modified systems discussed below successfully yielding the results discussed below. I understand that a POSITA is a hypothetical person. He is not a genius. He thinks along the lines of conventional wisdom. I understand that a POSITA is also a person of ordinary creativity, not an automaton (*see* Section VI), below, for qualifications of a POSITA). I also understand that in determining who would qualify as a POSITA, it is appropriate to consider criteria such as: (a) the type of problems encountered in the art; (b) prior art solutions to those problems; (c) the rapidity with which innovations are made; (d) the sophistication of the technology; and (e) the education level of active workers in the field. I understand that a given reference would have been relevant for a POSITA to consider if it came from the same field of endeavor or was reasonably related to a problem faced by the ’622 Patent inventors, and that

this relevance determination underlies a principle known as “analogous art,” which should be construed broadly.

24. **First**, turning to the types of problems and prior art solutions in the art, the “Field of the Invention” to the specification of the ’622 Patent states that the patent “relates to Internet communication, and more particularly, to improved data communication speed and bandwidth efficiency on the Internet.” EX1001, 1:23-25. The “Background” section further explains that the patent pertains to the increasing bandwidth required for video web sites for shopping news portals and social networks. *Id.*, 1:35-38. The ’622 describes two different prior art solutions to this problem, proxy servers which cache Internet content such as Akamai and peer-to-peer file sharing solutions such as BitTorrent.

25. **Second**, turning to the sophistication of the technology and the rapidity with which innovations occur in the field, the technical knowledge required to understand techniques to improved data communication speed and bandwidth efficiency on the Internet at the time of the alleged invention required education and experience in Internet communications technology to understand. For example, the ’622 Patent specifically discusses the knowledge of a POSITA in regards to HTTP, TCP/IP, IP addresses, and Request for Comments (“RFC”) 2616. *See* EX1001, 16:21-28, 17:20-24. A person skilled in the art would have been monitoring these developments.

26. **Third**, with respect to the educational level of active workers in the field, I personally observed that the individuals that participated in development and implementation of Internet routers/switches, network communication and Web servers typically have a bachelor's degree in Computer Science or related field (or equivalent experience), and at least two years' experience working with and programming networked computer systems.

27. **Fourth**, turning to the educational level of the named inventors, the '622 Patent names two inventors: Derry Shribman and Ofer Vilenski. I am not personally acquainted with any of these individuals, but I located information from their LinkedIn profiles that I reasonably believe to be associated with these individuals.

28. Derry Shribman's profile indicates that he has a bachelor's degree in Computer Science from the Open University and at least two years' experience working with and programming networked computer systems, including designing or implementing of Web, Internet, or network communication systems through with work companies including Cisco. <https://www.linkedin.com/in/derryshribman/details/experience/>

29. Ofer Vilenski's profile indicates that he has bachelor's degree in Computer Science or related field (or equivalent experience) from Israel Institute of Technology, and at least two years' experience working with and programming

networked computer systems, including designing or implementing of Web, Internet, or network communication systems through with work companies including Cisco. <https://www.linkedin.com/in/ofar-vilenski/>

30. I have not been asked to take a position on whether a given claim would have been legally obvious to a POSITA at the time of the alleged invention, but I have been told that some or all of my opinions are being used to support the argument that the claims of the '622 Patent are obvious.

31. I understand that a claim term is given the meaning that the term would have to a POSITA at the time of the invention, which generally is the ordinary and customary meaning of the term. I further understand that the ordinary and customary meaning of a term may be evidenced by a variety of sources, including the words of the claims themselves, the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art.

VI. LEVEL OF ORDINARY SKILL IN THE ART

32. I understand that the claims and specification of a patent must be read and construed through the eyes of a person of ordinary skill in the art ("POSITA") at the time of the earliest alleged priority date for the '622 Patent, October 8, 2009 ("Priority Date"). Unless otherwise stated, this declaration concerns the viewpoint of a POSITA with respect to the '622 Patent.

33. In my opinion, a person of “ordinary skill in the art” to which the ’622 Patent pertains would have had at least a bachelor’s degree in Computer Science or related field (or equivalent experience), and at least two years’ experience working with and programming networked computer systems, including designing or implementing of Web, Internet, or network communication systems. A POSITA would also have familiarity with the Internet Engineering Task Force (IETF) standards and protocols relating HTTP, TCP/IP, IP addresses. This definition is approximate, and more education may substitute for industry experience or vice versa.

34. In addition, in my opinion, while a person of ordinary skill in the art would have some familiarity with such underlying technologies, that familiarity would need only be sufficient to utilize the technology in connection with a broader system and method. For example, a person of ordinary skill in the art would be aware of how networked communication takes place over the Internet and how HTTP requests are processed in accordance to standards, but would not necessarily need to be an expert on the design of the Web servers or Internet caches.

35. Based on my educational and employment background, I am qualified to provide opinions concerning what a POSITA would have known and understood by October 8, 2009. Indeed, as reflected in my qualifications above, I am more than

qualified as a person of ordinary skill in the art as of the relevant date of the '622 Patent.

VII. OVERVIEW OF THE TECHNICAL FIELD & PRIOR ART

36. In this section, I describe the field of technology prior to the Priority Date of the '622 Patent in October of 2009. This would be indicative of the working knowledge of a POSITA at that time. Further, because the following discussion relates to Internet protocols, Internet communication, and proxies, this directly relates to the subject matter of the '622 Patent. Indeed, the '622 Patent specifically discusses the knowledge of a POSITA in regards to HTTP, TCP/IP, IP addresses, and even the IETF RFC 2616 (the standard for the HTTP/1.1 protocol, published in 1999), as I further discuss later in this Declaration. EX1005, 1/114.

A. RFC 2616

37. Web communications and routing were well-known prior to the Priority Date. For example, RFC 2616, which the '622 Patent recognizes “define[s]” “the HTTP protocol,” was published ten years earlier by the HTTP Working Group of the Internet Engineering Task Force (IETF) in June 1999. EX1001, 16:21-22; EX1005, 1/114. I obtained a copy of RFC 2616 from the IETF website source that I understand to be the repository of IETF’s RFCs, and which a POSITA would commonly utilize to obtain an electronic copy of the IETF’s RFCs. The copy of RFC

2616 that I obtained from <https://datatracker.ietf.org/doc/html/rfc2616> is attached as EX1005.

38. RFC 2616 explains that “the HTTP protocol is a request/response protocol” and that “most HTTP communication is initiated by a user agent [(UA)] and consists of a request to be applied to a resource on some origin server [(O)].” EX1005, 8/114. “HTTP communication usually takes place over TCP/IP connections.” EX1005, 11/114. RFC 2616 also confirms the role-based constructions for “client” and “server” as discussed in VIII.A are correct: “Any given program may be capable of being both a client and a server; *our use of these terms refers only to the role being performed* by the program for a particular connection.” EX1001, 16:21-22; EX1005, 8/114.

39. In addition to describing “client” and “server” operations, RFC 2616 discloses multi-hop routing using “proxy” devices running “intermediary program which acts as both a server and a client for the purpose of making requests on behalf of other clients.” EX1005, 8/114. That is, while communication may be “accomplished via a single connection (v) between the user agent (UA) and the origin server (O),” “more complicated situation[s]” were also known “when one or more intermediaries are present in the request/response chain,” such as an illustrated chain with “three intermediaries (A, B, and C).”

```

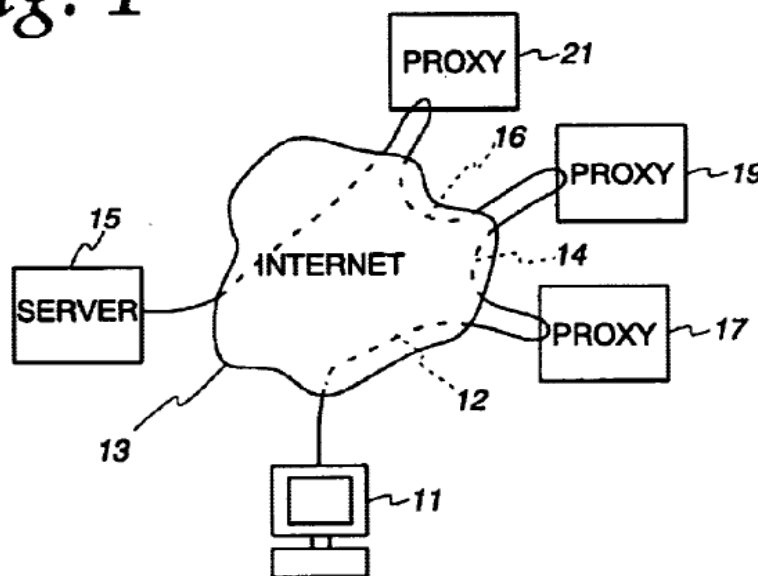
request chain ----->
UA -----v----- A -----v----- B -----v----- C -----v----- O
<----- response chain

```

Id., 10/114.

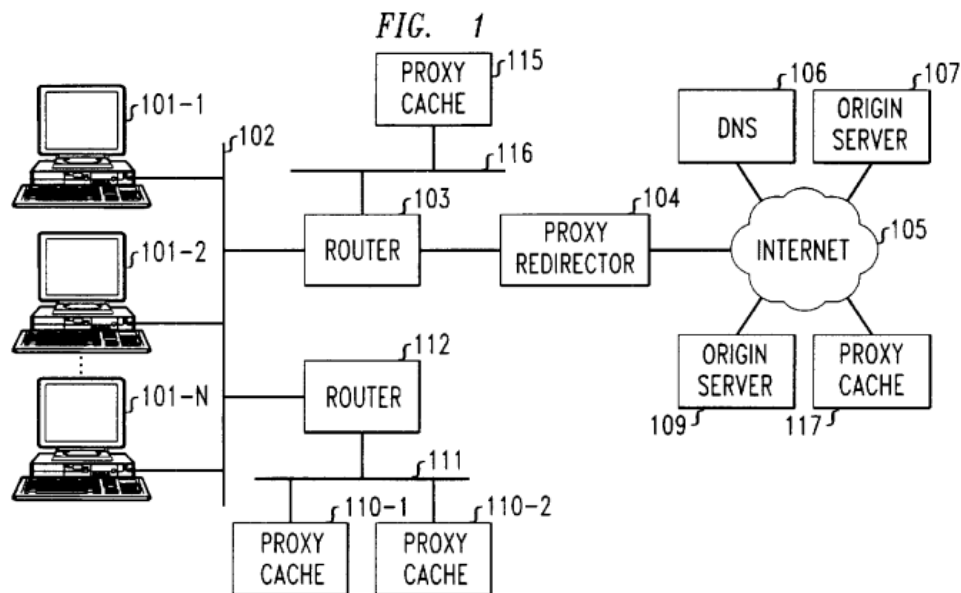
40. Prior art references, including Kocherlakota, confirm that it was well-known for an intermediary to determine routing of a received request based on that request. For example, Kocherlakota discloses proxy 17 receiving URLs from client computer 11 and selecting the IP address for forwarding to proxy 19, proxy 21, or web server 15 based on the URL. EX1003, 4:15-52, 5:18-24.

Fig. 1



Id., FIG. 1.

41. Likewise, Cohen discloses “proxy redirector 104” intercepting web requests from “client 101-1” and “select[ing] one of the available proxy caches to which to forward client requests based ... IP header information such as the origin server IP address.” EX1004, 7:36-48; FIG. 1.



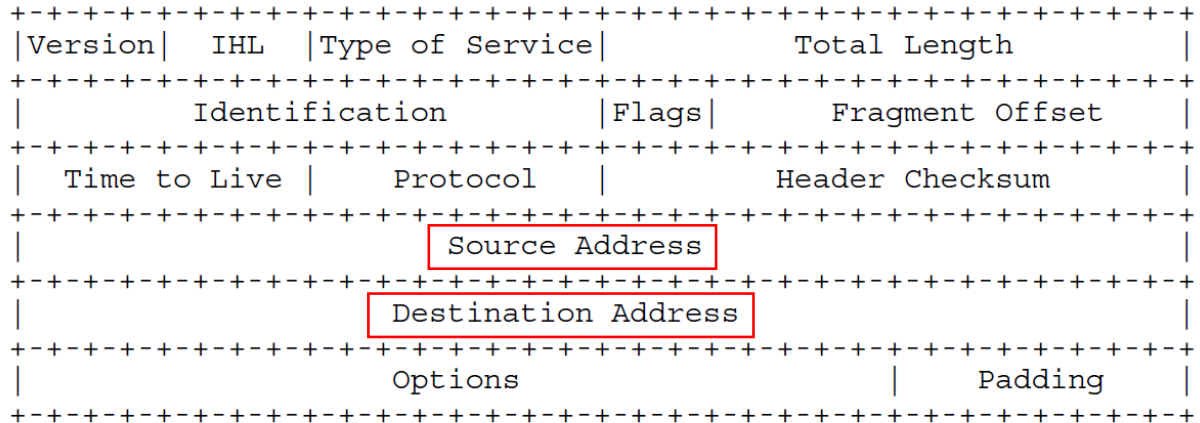
Id., FIG. 1.

B. RFC 791

42. HTTP’s relationship to other well-known Internet standards was also known. For example, IP is an example of a well-known Network Layer protocol. In particular, IPv4 was published as an Internet Standard in RFC 791 in September 1981. This RFC serves as the informational drafts and formal standards for many Internet protocols, and are published by the Internet Engineering Task Force (IETF).

RFC 791's front page indicates that it is a September 1981 publication that served as the "DARPA Internet Program Protocol Specification" for the "Transmission Control Protocol." EX1015, 1. It was posted on the Internet and published in the ordinary course by the IETF, and was meant to be viewed by the interested Internet engineering audience at large as of its date of publication stated on its cover. I obtained a copy of RFC 791 from the IETF website source that I understand to be the repository of IETF's RFCs, and which a POSITA would commonly utilize to obtain an electronic copy of the IETF's RFCs. The copy of RFC 791 that I obtained from <https://datatracker.ietf.org/doc/rfc791/> is attached as EX1015.

43. The IP protocol (such as described in IPv4) describes a set of rules for defining a IP packet format, including a header with network source and destination address information, and a datagram body (some fixed-maximum-length message), and then transmitted those IP packets from an IP sender to an IP destination across links in a computer network. As shown below, IP Packets include a header that includes a "source address" and "destination address":



Example Internet Datagram Header

Figure 4.

EX1015, 17/51; *see also* EX1016, 57/91 (in TCP, “[a]ny lower level protocol will have to provide the source address, destination address”).

44. The datagram body, or message, carried within a single IP packet typically has a maximum length of around 1500 bytes, which corresponds to a few paragraphs of text. EX1015, 13/51. The IP protocol only offers “best effort” delivery of IP packets: An IP sender can transmit an IP packet to an IP recipient (based on the IP addresses of sender and recipients that are in the packet’s headers), and the various networking routers will “attempt” to forward the packet to its proper destination, but the packet can be arbitrarily corrupted, dropped, or delayed. Because of this, when multiple IP packets belonging to the same “stream” – such as part of a web transfer between a webserver and a web browser – are sent from a sender to

recipient, the recipient may only receive some of the packets (others may be lost) and the packets may be received “out of order” from when sent (because some packets were delayed by the network or took a different path through the network than others). These limitations by the IP layer in providing a “reliable stream” are solved by the TCP protocol.

C. RFC 793

45. The TCP protocol has also been well-known to a POSITA for quite some time, having been standardized in September 1981 in the IETF RFC 793. EX1016. RFC 793’s front page indicates that it is a September 1981 publication that served as the “DARPA Internet Program Protocol Specification” for the “Transmission Control Protocol.” EX1016, 1. It was posted on the Internet and published in the ordinary course by the IETF, and was meant to be viewed by the interested Internet engineering audience at large as of its date of publication stated on its cover. I obtained a copy of RFC 793 from the IETF website source that I understand to be the repository of IETF’s RFCs, and which a POSITA would commonly utilize to obtain an electronic copy of the IETF’s RFCs. The copy of RFC 793 that I obtained from <https://datatracker.ietf.org/doc/rfc793/> is attached as EX016.

46. TCP serves as a transport layer that makes the “best effort” packet delivery of the IP layer more usable by applications, such as Web browsing using

HTTP. Specifically, TCP, builds on and adds functionality to the lower-level IP network layer by segmenting the stream of data is segmented into individual fixed-sized segments, where each segment is carried within a separate IP packet. Each segment is also associated with a sequence number, which allows a receiver to place IP packets that are received out-of-order back into the proper stream order. The sequence numbers also help receivers understand if certain segments are missing, and they subsequently can re-request missing segments from the sender, who retransmits these missing segments in order to ensure reliable delivery. As a result, most Internet traffic uses TCP as a reliable, stream-based protocol that runs on top of IP networks. For these reasons, Internet traffic is often described as “TCP over IP” or simply “TCP/IP.” When that traffic happens to also use HTTP as the application layer protocol, it is often described as “HTTP over TCP/IP.” *See* EX1005, 11/114 (stating that “HTTP communication usually takes place over TCP/IP connections”); EX1001, 17:20-26 (describing “TCPIP” as “known” and referencing a “Web server” that “is a TCPIP server”).

47. TCP also provides connection management, reliable retransmission, reordering, and other features like flow and congestion control as a component in the operating systems running on the sender and receiver, such as the web server and web browser. TCP is thus implemented on basically every common operating system, including Microsoft Windows, Apple Mac OS (including iOS running on

iPhones), Linux (including Android for mobile), the BSD operating system, and every UNIX variant. *See* EX1016, 14/191 (stating that “TCP is assumed to be a module in an operating system. The users access the TCP much like they would access the file system. The TCP may call on other operating system functions, for example, to manage data structures. The actual interface to the network is assumed to be controlled by a device driver module. The TCP does not call on the network device driver directly, but rather calls on the internet datagram protocol module which may in turn call on the device driver.”).

48. Finally, advanced features of TCP (as discussed below) were also known, notably the use of a “‘keep-alive’ mechanism” “[t]o confirm that an idle connection is still active.” EX1006, 102/116.

VIII. CLAIM CONSTRUCTION

49. For purposes of this IPR proceeding, I apply the common and ordinary meanings of claim terms in the ’622 Patent, unless otherwise noted. For example, I note that the Court issued three claim construction orders in the related litigation construing terms of the ’511, ’968, ’319, and ’510 Patents, which have the same specification and share claim language with the Challenged Claims, and are relevant to construction of the Challenged Claims.

50. I specifically discuss certain claim terms below.

A. “Client Device” and “First Server”

51. The Challenged Claims use the same “client device” and “first server” terms as the claims of the ’511 Patent and related patents. EX1011, 5/37; EX1010, 3-4/24. Across three Orders the Court repeatedly confirmed that “client” and “server” refer to the role the device plays, not any hardware characteristics or label.

52. In each of the *Teso* (for the ’319 and ’510 Patents) and *Code200* (for the ’511 and ’968 Patents) Orders, the Court held that “client device” means “communication device that is *operating in the role of a client*” and rejected PO’s contention that the term required a “consumer computer.” EX1010, 10-12/24; EX1011, 11-13/37.

53. As to “first server,” in the *Code200* Order, the Court addressed “whether one component can simultaneously serve as more than one of: the client device, the first server[], and the web server,” concluded “[i]t cannot,” and construed “first server” as “server that is not the client device or the web server.” EX1011, 13-15/37. Subsequently, it became apparent that “server” required further construction, and Petitioner requested a clarified construction of: “a device that is operating in the role of a server and that is not the first client device or the web server.” EX1012, 2/5 (emphasis in original). The District Court declined to formally change the construction, but confirmed “Defendants’ understanding of the scope of the construction[], as *represented by the requested clarification*[] ..., *is correct*” and

“already embedded in” the original construction. EX1013, 7-11/12. The Court confirmed that “a component can be *configured* to operate in different roles—so long as it does not ‘simultaneously serve as more than one of: the client device, the first server/second server, and the web server.’” *Id.*, 10/12 (emphasis in original).

54. RFC 2616, which the ’622 Patent confirms “define[s]” “the HTTP protocol,” further confirms that the role-based constructions are correct: “Any given program may be capable of being both a client and a server; ***our use of these terms refers only to the role being performed*** by the program for a particular connection.” EX1001, 16:21-22; EX1005, 8/114.

55. RFC 2616 also provides further guidance on each of these “roles,” defining a “client” as “establish[ing] connections for the purpose of sending requests” and a “server” “accept[ing] connections in order to service requests by sending back responses.” EX1005, 8/114. RFC 2616 explains that a “proxy,” the component of Kocherlakota and Cohen mapped to various claim elements, is an “intermediary program which ***acts as both a server and a client*** for the purpose of making requests on behalf of other clients.” EX1005, 8/114. These RFC 2616 statements would have carried significant weight with a POSITA.

B. “Selecting, in response to the receiving of the [first / second] URL”

56. In the *Tefincom* Litigation, Defendant asserted that PO was inconsistently applying this term, assuming for purposes of infringement that “in

response to the receiving” was met by performing the selection “upon receiving,” while assuming for purposes of invalidity that the selecting must take into account the contents of the received URL (“content identifier” in the ’511 Patent claims). EX1014, 6/20. The Board need not reach this dispute as each of Petitioner’s mappings demonstrate the art discloses the narrower construction, taking into account the contents of the received URLs.

C. “First server” “sending ... to the [first / second] web server using the selected IP address”

57. While the claim language recites the first server sending **to** the web server, dependent Claims 3 and 4 recite that this step is met by the first server sending the URL not to the web server, but to an intermediary with the intermediary then sending to the web server. EX1001, Claims 3-4. Accordingly the Court construed this language as “sending . . . the first content identifier to the web server using the selected IP address as either a sending address or a receiving address,” and “clarifies that the Court’s construction does not exclude intermediaries specifically with respect to ’511 Patent Claims 2–5.” EX1013, 7-12.

D. “... using the selected IP address as a source address”

58. PO asserted in *Code200* that this language, which is found in dependent Claim 25 of the ’511 Patent, refers to “the IP address of the sender of a communication” and “not the IP address of the web server” (“**PO Construction**”).

EX1013, 2/13. The Court disagreed, holding that the specification “suggests that ‘source’ is used to refer to a *content* source rather than a *communication* source” and thus held that “‘source address’ is reasonably limited to the address of the source of content, which in Claim 1 is the web server” (“**Court Construction**”). *Id.*, 2-5/12. The Petition applies both constructions.

IX. THE '622 PATENT

59. The '622 Patent specification describes system of caching proxies to “improv[e] data communication speed and bandwidth efficiency on the Internet.” EX1001, 1:24–25. FIG. 3 of the '622 Patent, copied below, depicts “peer[s],” a “client,” and an “agent” communicating, with the “agent” forming a connection to the web server 152.

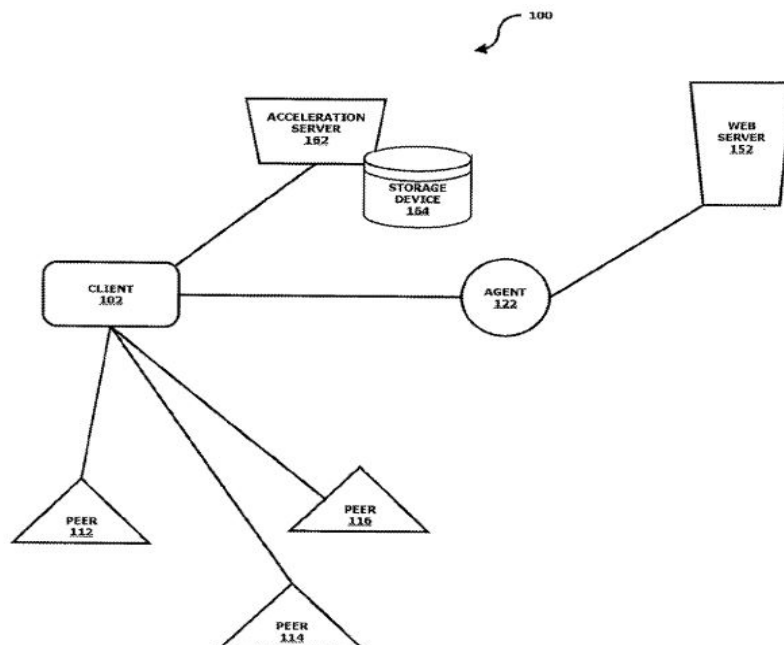


FIG. 3

60. To initiate communications, the client 102 sends a web request to acceleration server 162, which responds with a list of agents that may assist. *Id.*, 5:10-19, 13:8-22. Client 102 then contacts agent 122, which responds with a list of peers that have cached the requested web page, and client 102 contacts an identified peer to obtain the content. *Id.*, 13:62-64, 14:13-58, 15:14-20. The only device disclosed as contacting a web server is agent 122, which does so only when agent 122 does not identify any peers with cached content. *Id.*, 14:62-15:6. In that case, agent 122 directly contacts the web server, obtains the content, and responds to client 102 identifying itself as the only available peer—there is no “selecting” by either client 102 or agent 122 in this process. *Id.*, 15:6-11.

61. With respect to FIG. 3, the patent states “[t]he network 100 of FIG. 3 contains multiple communication devices,” that “*each communication device may serve as a client, peer, or agent*,” and that “a detailed description of a communication device is provided with regard to the description of FIG. 4.” *Id.*, 4:44-53 (emphasis added). The patent specification confirms that standard, off-the-shelf features of the “communication device,” including that the “communication device 200 includes a processor 202, memory 210, at least one storage device 208” *Id.*, 5:59-60. The specification also confirms other standard features of the “communication device,” including that its memory may include “ROM, hard drive, tape, CDROM, etc.” and that its input/output devices may include “a keyboard,

mouse, scanner, micro-phone, etc.” or a printer. *Id.*, 6:14-24, 6:61-7:3. Each communication device is also comprised of a “cache database 282,” that:

“stores responses to HTTP requests that the communication device 200 has dispatched . . . the responses to HTTP requests are stored within the cache database 282 for future use by this communication device 200, or for other communication devices within the communication network 100 that need to retrieve this information and will use this communication device as either a peer or an agent.

Id., 8:10-20; *see also Id.*, 7:60-8:4, 8:24-37, 9:60-10:21, 10:47-60, 11:4-11, and Fig. 7.

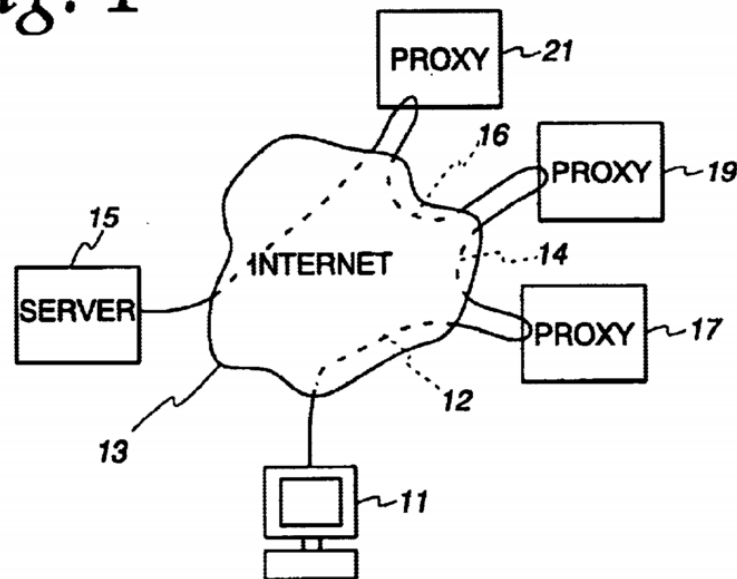
62. The '622 Patent concludes with independent claim 1 and dependent claims 2 – 32.

X. OVERVIEW OF PRIOR ART REFERENCES

A. U.S. Pat. No. 6,785,705 (“Kocherlakota”) EX1003

63. Kocherlakota “relates to the use of web proxy servers by internet clients and more particularly, to the use of multiple such proxies contemporaneously.” EX1003, 1:7-9. FIG. 1 “shows an internet connection through a plurality of chained proxies.” *Id.*, 2:39-40.

Fig. 1



64. The client computer 11 is connected to the Internet for accessing content from web servers by sending URLs. (“the client can access the internet by sending URLs ...) *Id.*, 2:5-6. Web server 15 of FIG. 1 represents all addressable web servers on the Internet.

(“FIG. 1 is a web server 15 which is representative of any of 60 the well known data file providers and, in fact, represents the universe of addressable web servers.”) *Id.*, 2:59-61.

65. Client computer 11 can make use of proxy services provided by proxies 17, 19 and 21, while accessing the Internet content. Such services include anonymity services, language services or wait limiting services.

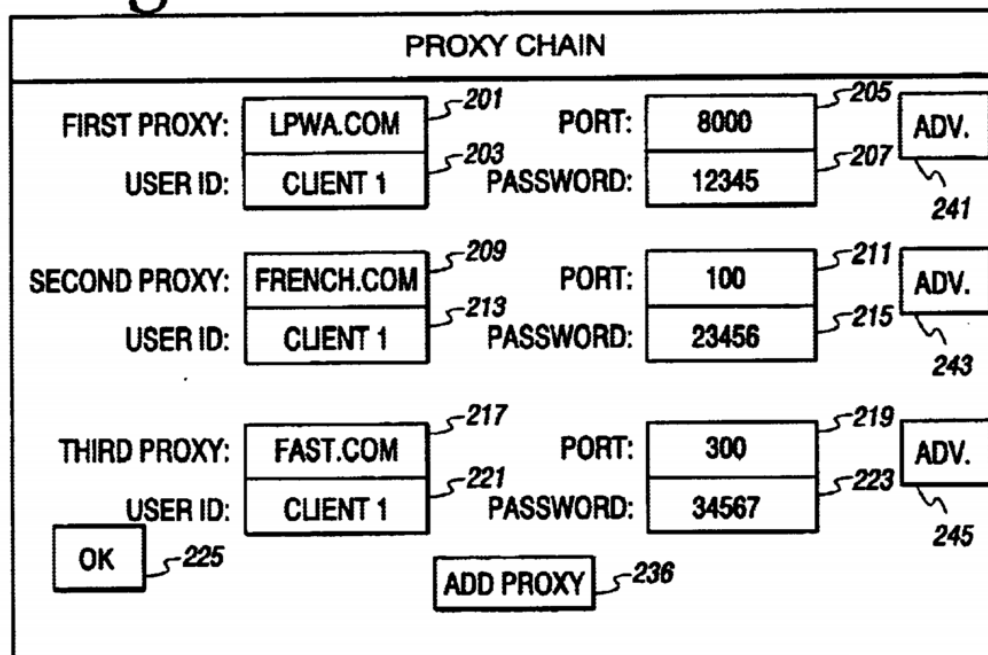
(“Client 11 desires to take advantage of services provided by a plurality of web proxies. For example, the client wants to be anonymous so a connection via an **anonymity web proxy 17 is desirable**. Also, the client would like to search in the French language and therefore wants to take advantage of the **language service provided by a French language web proxy 19**. Lastly, the client would like to reduce the amount of time spent retrieving data so the **services of a wait limiting proxy 21** are desired.”) *Id.*, 2:61 – 3:3.

66. To use these services while accessing content from Web servers, the client computer makes use of an applet provided by a proxy server. Proxy 17 transmits an applet to the client which provides a GUI interface for the client that presents a number of information lines into which the client can enter identities of proxy servers.

(“The client first sends out the URL of the first proxy server 17 for anonymity services in step 101 of FIG. 3. Proxy server 17 receives the contact from client 11 and establishes a session (step 109, FIG. 4) between the client and proxy 17. As a part of the session, web proxy 17 returns an applet to 25 client 11 where it is executed as is well known. The applet, which is received and executed in a step 103 (FIG. 3) presents a window as shown in FIG. 2, on the client computer. The applet window presents a number of information lines

into which the client can enter identities of up to three proxy servers,..”) *Id.*, 3:20-33.

Fig. 2



67. When as shown in FIG. 2, the user identifies a second and third proxy, “the first proxy” receives the configuration information from the applet “and begins to establish sessions with the additional proxies.” *Id.*, 4:43-45.

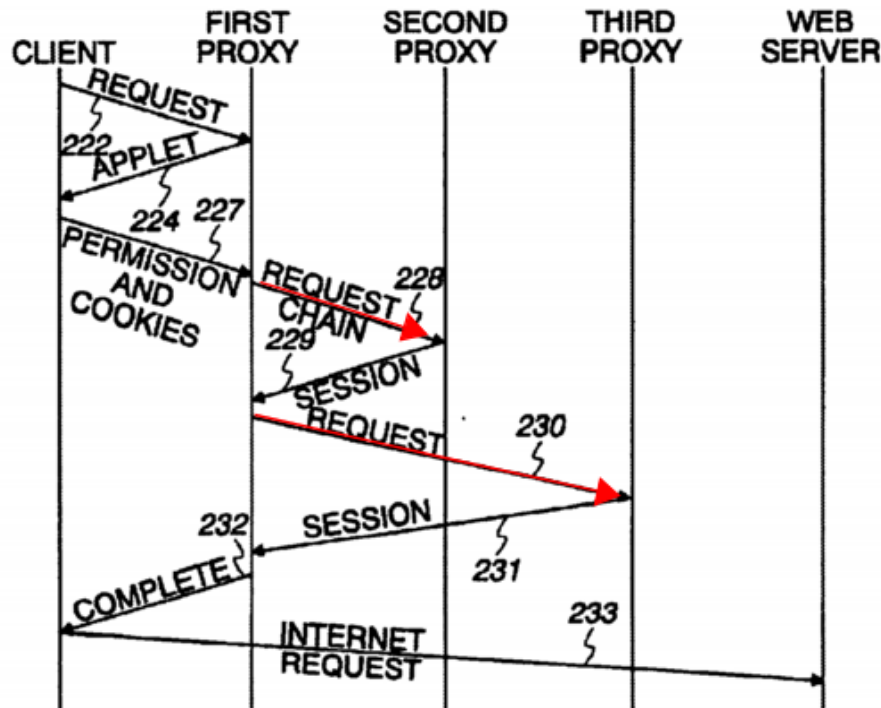
68. Specifically, proxy 17 sends a request to the second proxy which authenticates it and returns a message to the first proxy signifying the session establishment. The first proxy then sends a message to the third proxy requesting a

session. The third proxy responds by returning a session message to the first proxy, signifying the establishment of another session. In this way, the proxy server 17 is connected to second and third proxies with sessions.

(“The identities and permission data are then sent 227 to the **first proxy** which parses the message and **begins to establish sessions with the additional proxies**. A request is sent 228 to the second proxy which authenticates it and returns a message 229 to the first proxy signifying the session establishment. **The first proxy** then sends a message 230 to the **third proxy requesting a session**. The third proxy responds by returning a Session message 231 to the first proxy and the first proxy signifies 232 to the client that the chain is complete.”) *Id.*, 4:42:52.

(“In step 113 the **proxy 17 contacts the named second proxy server, i.e., french.com, to establish a session therewith**. The contact is received in step 119 (FIG. 5) and a session will be established in Step 121 using the client provided applet response information for the second proxy as well as the cookie from the client computer 17 relating to french.com. This session is maintained in step 125. **The first proxy server 17 then identifies in step 115 whether a third proxy** has been named in the applet response information (FIG. 2).”) *Id.*, 4 2-11.

Fig. 6



EX1003, FIG. 6 (annotated)

69. With these sessions established, web server 15 is accessed through a chain of proxies, proxy 17, 19 and 21.

(“After the proxy chain has been established, the URL of web server 15, or any other web server, can be sent from the client to the internet via the chained proxies 17, 19 and 21. The proxy 17 provides the necessary anonymity to the chain, the language proxy 19 provides the French language features and the wait avoidance proxy 21 provides its function for packets transmitted on the chain.) *Id.*, 4:29-35.

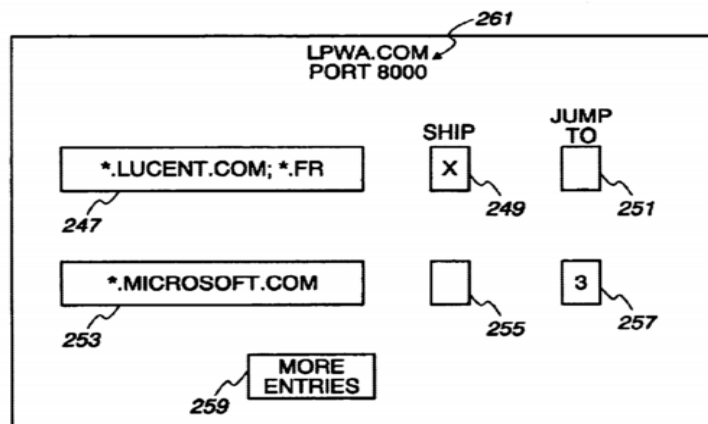
70. Kocherlakota also teaches more advanced routing of URLs to web proxies.

(“The preceding example of FIG. 2 relates to the standard features of proxy chaining. The chaining applet may also provide advanced features to the users who want to take advantage of them.”) *Id.*, 4:55-58.

71. With these advanced features, proxy 17 can route URLs to particular proxy servers, 19 or 21 depending on the particular URL and user configuration information. FIG. 7 shows how the user defines this URL and configuration information for the first proxy, LPWA.com.

(“The window of FIG. 7 relates to the first proxy **lpwa.com** which name and port number are displayed at 261. The window initially presents to the user two rows of text windows and control boxes.”) *Id.*, 5:3-7.

Fig. 7



72. With the window of FIG. 7, a user can define advanced features to apply to specific predetermined URLs. A specific URL can cause the first proxy to execute a “skip” or “jump to” command.

(“The text window 247 is used to enter URL's for which the first proxy is to be skipped or a “jump to” command is to be entered.”) *Id.*, 5:9-11.

73. As shown in FIG. 7, proxy 17 can be configured to have the services of LPWA.com skipped for specific predetermined URLs, such as *.LUNCENT.COM or *.FR.com, if box 249 is checked. The asterisk represents well-known matching criteria for text strings, and are particularly known as “wildcards” which can match one or more characters.

(“As shown in FIG. 7, when a URL matching *.lucent.com or *.fr is transmitted to the first proxy, the services of that proxy are to be skipped as defined by the “X” in box 249.”) *Id.*, 5:17-21.

74. Also, as shown in FIG. 7, proxy 17 can be configured to jump to the third proxy and skip the second proxy entirely for specific predetermined URLs, in this case *.Microsoft.com or *.companyx.com.

(“Similarly, whenever a URL of *.**companyx.com** is sent to the first proxy, the first proxy will **skip the second proxy and jump to the third proxy** because the number 3 is entered into the jump to box 251.”) *Id.*, 5:21-24

75. In this way a user can define which proxy servers are used for specific predetermined URLs.

(“The advanced features allow the user to **define which proxy 25 servers are employed for predetermined URLs.**”) *Id.*, 5:24-26.

76. Thus, Kocherlakota teaches a number of ways URLs will be routed by proxy 17. If advanced features are not used, i.e. a URL is not predetermined, as it does not match any URL in the windows of FIG. 7, the URL will be sent via the chained proxies 17, 19, and 21. That is, the URL will be sent by proxy 17 to proxy 19. If the URL matches the skip criteria, this URL will be directly sent to proxy 19. If the URL matches the criteria of a “jump to” URL, proxy 17 will skip all the proxy servers and jump to the proxy server designated in “jump to” box.

77. A POSITA would understand that the session setup and maintenance of these sessions, as well as the routing of URLs through different proxy servers to web servers, necessarily requires, or at a minimum renders obvious, proxy 17 storing a group or list IP addresses of proxies 19 and 21 as well as client computer 11. If these addresses were not stored, then proxy 17 would have no way of creating a message to send to the intended receivers over the Internet. As a POSITA would understand, the Internet makes use of IP packets, which make use of IP addresses to establish sessions and send messages over the sessions. Kocherlakota confirms this understanding.

(“An anonymity proxy **establishes a session with a client using the client’s IP address** and user information and requests information from the internet without identifying the requesting client.”) *Id.*, 1:24-27.

78. Thus, in order for proxy 17 to establish and maintain sessions with proxies 19 and 21, proxy 17 would have and store the IP address corresponding to the domain name of the other proxy servers (e.g., “french.com”, “fast.com”) that the user enters for proxies 19 and 21, otherwise proxy 17 could not establish a session with these proxies over the Internet. Likewise, to establish and maintain sessions with client computer 11 over the Internet, proxy 17 must store the IP address of client computer 11, which would be received as the “sending address” when client computer 11 contacts proxy 17.

79. Furthermore, a POSITA would understand that the proxy 17 must also subsequently store and make use of these IP addresses so that the sessions between proxy servers remain active. Accordingly, when proxy 17 selects proxy 19 or 21 for routing based on the received URL, proxy 17 selects the IP address of the proxy from the group of proxy IP addresses that are stored in order to route to that proxy. If for some reason the session became inactive, a POSITA would understand that there are well-known techniques to convert a URL of the proxy server into an IP address using DNS. *See e.g.* EX1005, 94/114 (“clients using HTTP rely heavily on the Domain Name Server...”).

80. Kocherlakota was issued by the USPTO on August 31, 2004. Kocherlakota thus predates the earliest claimed priority date for the '622 Patent, October 8, 2009. Therefore, I understand Kocherlakota to qualify as prior art.

B. RFC 1122

81. RFC 1122 is titled “Requirements for Internet Hosts – Communication Layers” and provides requirements for link layer, Internet layer, and transport protocols over the Internet. This RFC is a one of a pair of RFCs, which define the requirements of Internet host software, the other being RFC 1123, which is listed as a reference in RFC 2616. *See* EX1005, 97/114. RFC 1122 was published twenty years before the '622 Patent's priority date by the Network Working Group of the Internet Engineering Task Force (IETF) in October 1989. Applicants submitted RFC 1122 to the Patent Office during prosecution of the '622 Patent. EX1007, 1250/1467 (Information Disclosure Statement listing RFC 1122 as prior art). RFCs (and similar standards documents) posted on the Internet are published in the ordinary course by established standards organizations, and are intended to be viewed by the interested Internet engineering audience at large as of their dates of publication as stated on the cover of each. Therefore, I understand RFC 1122 to qualify as prior art.

82. I obtained a copy of RFC 1122 from the IETF website source that I understand to be the repository of IETF's RFCs, and which a POSITA would commonly utilize to obtain an electronic copy of the IETF's RFCs. The copy of RFC

1122 that I obtained from <https://datatracker.ietf.org/doc/html/rfc1122> is attached as EX1006.

83. RFC 1122 describes various features of the TCP protocol and in particular describes a “keep alive” mechanism to confirm that TCP connections are still active. As described in RFC 1122, this keep alive mechanism periodically probes the other end of a connection when the connection is otherwise idle, even when there is no data to be sent.” EX1006, 102/116. “To confirm that an idle connection is still active,” some TCP “implementations send a probe segment designed to elicit a response from the peer TCP.” *Id.* “[T]he probe causes the receiver to return an acknowledgment segment, confirming that the connection is still live. If the peer has dropped the connection due to a network partition or a crash, it will respond with a RST instead of an acknowledgment segment.” *Id.*

C. U.S. Pat. No. 6,389,462 (“Cohen”)

84. Cohen discloses a system and method for intercepting client web requests and redirecting them to proxy caches. EX1004, 1:7-9. The proxy cache has a stored copy of the object on the origin server.

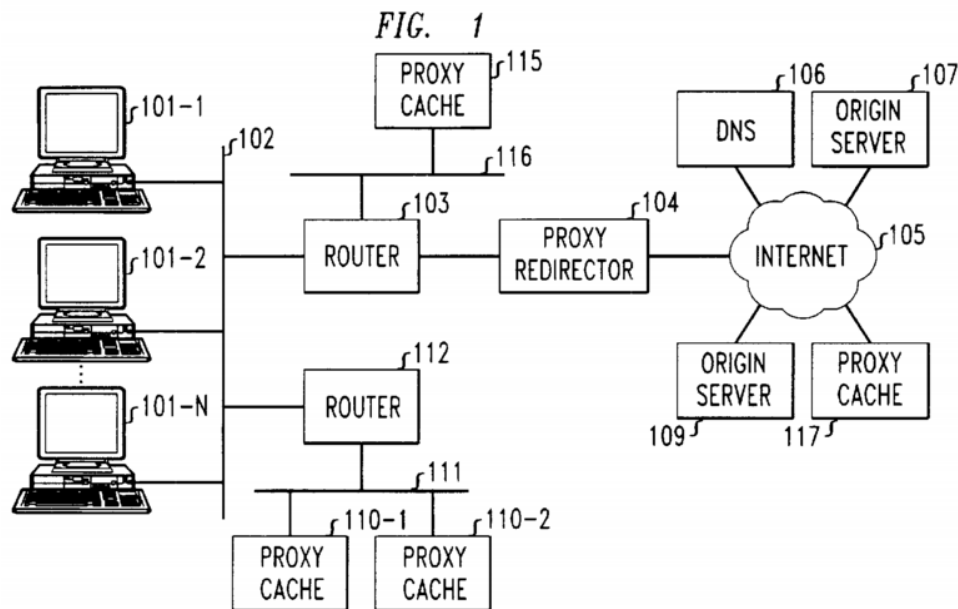
(“Proxy caching is currently used to decrease both the latency of object retrieval and traffic on the Internet backbone. **As is well known, if a proxy cache has stored a copy of an object from an origin server that has been**

requested by a client, the requested object is supplied to the client from the proxy cache rather than from the origin server.”) EX1004, 1:13-18.

85. The process described in Cohen begins when a client makes a request with a URL through a web browser, which initiates a DNS lookup which returns the associated IP address.

(“When any of the clients connected to LAN 102, such as **client 101-1**, makes a request through a browser for an object **by specifying a logical URL**, a **domain name server** (DNS) 106 connected locally or on Internet 105, as shown, is accessed to perform a database look-up based on that logical name. An associated **IP address is then returned to the browser.**”) *Id.*, 6:47-54;
(“That IP address then serves as the IP address to which packets directed to the origin server from the client are directed.”). *Id.*, 6:55-65.

86. Then according to the invention, “once the IP address of the origin server corresponding to the logical URL name is determined through the DNS look-up, **proxy redirector 104**, rather than establishing a TCP connection to the origin server at the determined IP address, **transparently establishes a TCP connection between the client and a proxy**. If the requested object is stored in the cache, a copy of that object is transparently returned to the requesting client.” *Id.*, 7:12-19; FIG. 1 below.



87. Specifically, the “proxy redirector 104” intercepts a web request from a “client 101-1” seeking content from a target web server and “selects one of the available proxy caches [e.g. 110-1, 110-2, 115, and 117] to which to forward client requests based on a metric such as least-loaded or round-robin, [or] based on IP

header information such as the origin server IP address.” EX1004, 7:36-48; see also *Id.*, 2:15-20.

88. Cohen teaches that after the TCP connection is established, the client sends “one or more packets to the origin server [via the proxy redirector 104], which packets include a GET request. The GET request includes a complete URL, which identifies to that server the specific object within the origin server site that the client wants a copy of.” *Id.*, 9:19-22.

89. The proxy redirector 104 then forms the absolute URL by prefixing the complete URL “with the IP address of the origin server obtained from the destination IP address of the packet(s) containing the GET request.” *Id.*, 9:28-10:3. “Responsive packets from the proxy cache are sent to proxy redirector 104 where they are redirected to client.” *Id.*, 8:55-58. “If the proxy cache to which the request is directed does not contain the requested object, a separate TCP connection is established between the proxy cache and the origin server to obtain a copy of the requested object.” *Id.*, 7:27-35.

XI. COMPARISON OF THE PRIOR ART TO THE CLAIMS

90. I understand claims are to be given their ordinary and customary meaning to a POSITA in view of the claims, specification, and prosecution history. I also understand that Applicants can define their own claim terms in the specification, which will be used when interpreting the claims.

A. Ground 1 – Kocherlakota Renders Obvious Claims 1-7, 10, 14, 16-17, 20-24, 26-32

1. Claim 1

- a. Limitation 1[p]: A method for fetching, by a first client device, a first content that comprises a web-page, an audio, or a video content, and is identified by a first Uniform Resource Locator (URL) and stored in a first web server, for fetching, by the first client device, a second content that comprises a web-page, an audio, or a video content, and is identified by a second URL and stored in a second web server, for use with a first server that stores a group of IP addresses, the method by the first server comprising**

91. In my opinion, Kocherlakota discloses or renders obvious this limitation. Kocherlakota teaches fetching, by a first client device, content from a web page is identified by a first URL. Kocherlakota teaches client 11 fetching content identified by the URL is stored in web server 15.

(“After the proxy chain has been established, the URL of web server 15, or any other web server, can be sent from the client to the internet via the chained proxies 17, 19 and 21”) EX1003, 4:29 – 31.

92. Kocherlakota discloses fetching, by the first client device, a second content that comprises a web-page, an audio, or a video content, and is identified by a second URL and stored in a second web server for use, as it teaches that web server

15 represents the universe of all addressable web servers which would all have different URLs.

(“Also, shown in FIG. 1 is a web server 15 which is representative of any of the well known data file providers and, in fact, represents the universe of addressable web servers.”) *Id.*, 2:58-61.

93. Kocherlakota therefore teaches Client computer 11, (first client device) fetches a web page identified by a first URL (containing the claimed “first content”) through proxy 17 (the claimed “first server”) as well as a different web page identified by a second URL (containing the claimed “second content”) through proxy 17.

94. The first URL is for example, a URL for which, by applying the logic shown in FIGs. 2 and 7, proxy 17 selects proxy 19. As described above in Section X.A, ¶¶70-76, Kocherlakota teaches a number of ways URLs will be routed by proxy 17. If advanced features are not used, i.e. a URL is not predetermined, as it does not match any URL in the windows of FIG. 7, the URL will be sent via the chained proxies 17, 19, and 21. That is this URL will be sent by proxy 17 to proxy 19. If the URL matches the skip criteria, this URL will be directly sent to proxy 19.

95. Also as described above in Section X.A, ¶74, a second URL is a URL for which, by applying the logic shown in FIGs. 2 and 7, proxy 17 selects proxy 21. For example, upon receiving www.microsoft.com for example, proxy 17 would

select proxy 21 because the web page corresponding to this URL matches the criteria in text window 253 and the “jump to” command 257 with “3” was entered.

96. Also as described above in Section X.A, ¶¶77-79, a POSITA would understand that the session setup and maintenance these sessions, as well as the routing of URLs through different proxy servers to web servers, necessarily requires, or at a minimum renders obvious, proxy 17 storing a list or group of IP addresses associated with proxies 19 and 21 and client computer 11.

97. Client computer 11 meets the construction of “client device” because it is a device that communicates over the Internet and it is operating in the role of a client by establishing a connection with proxy 17 to make requests. EX1003, 2:54-58 (“client computer 11 connected to the internet 13”), 4:29-31 (“the URL of web server 15, or any other web server, can be sent from the client to the internet via the chained proxies 17, 19 and 21”). *See also id.*, 1:43-45, 2:4-7, 2:30-32.

98. Proxy 17 meets the construction of “first server” because it is a device operating in the role of a server by accepting a connection from client computer 11 to service requests (URL’s) by sending back responses (content from the web server) and because it is not the same physical device as client computer 11 (the claimed “first client device”). *Id.*, 5:3-24.

b. Limitation 1[a]: receiving, from the first client device, the first URL

99. In my opinion Kocherlakota discloses or renders obvious this limitation. Kocherlakota teaches proxy 17 receives the first URL from the client 11.

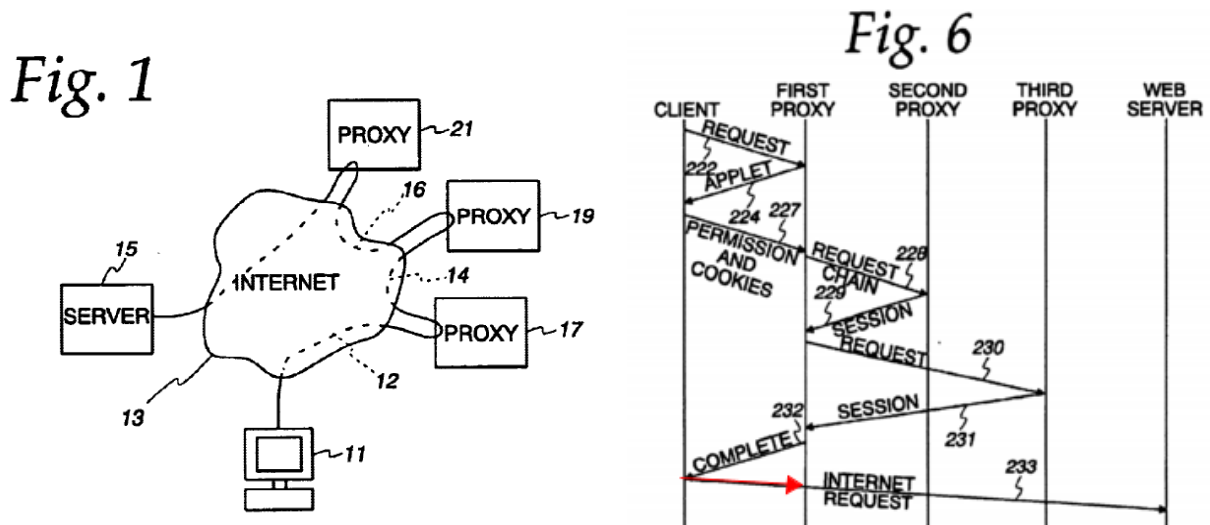
(“After the proxy chain has been established, **the URL of web server 15, or any other web server, can be sent from the client to the internet via the chained proxies 17, 19 and 21**”) EX1003, 4:29 – 31.

(“FIG. 1 includes dotted line segments 12, 14 and 16 and solid line 'loop' segments connecting each web proxy 17, 19 and 21 to the internet. These segments are functional in nature and illustrate the chained **connection of the client 11 to the web server 15 via the chained proxies 17, 19 and 21.**”) *Id.*, 3:3-8

100. By way of example, Kocherlakota teaches that the URL *.lucent.com is transmitted to proxy 17.

(“As shown in FIG. 7, when a **URL matching *.lucent.com or *.fr is transmitted to the first proxy**, the services of that proxy are to be skipped as defined by the “X” in box 249.”) *Id.*, 5:18-21.

101. FIG. 1 and FIG. 6 annotated below also show this disclosure.



c. **Limitation 1[b]: selecting, in response to the receiving of the first URL from the first client device, an IP address from the group**

102. In my opinion, Kocherlakota discloses or renders obvious this limitation. Kocherlakota teaches that Proxy 17 (the claimed “first server”) selects the IP address from the group of IP addresses for proxies 19 or 21 to route the URL through the proxy chain.

(“As shown in FIG. 7, when a **URL matching *.lucent.com or *.fr** is transmitted to the first proxy, the services of that proxy are to be skipped as defined by the “X” in box 249. Similarly, whenever a **URL of *.companyx.com** is sent to the first proxy, the first proxy will skip the second proxy and jump to the third proxy because the number 3 is entered

into the jump to box 251. The advanced features allow the user to define which proxy servers are employed for predetermined URLs.”) EX1003, 5:18-26.

103. As discussed in Section X.A, ¶¶70-76, upon receiving the URL, proxy 17 (the claimed “first server”) selects the IP address of either proxy 19 or 21 from the group of those IP addresses to route the URL through the proxy chain. This selection is “in response to the receiving of the first URL” because the selection of the URL is based on analysis of the URL performed by proxy server 17.

104. When proxy 17 receives from the client computer 11 a URL not matching the criteria in either text window 247 or 253, including www.uspto.gov, proxy 17 will not “skip” or “jump to” any server in the proxy chain because the URL does not match the criteria and will therefore select the IP address of the next proxy in the chain (i.e. proxy 19) so that the request passes “via the chained proxies 17, 19 and 21.” EX1003, 4:29-31, FIGs. 6-7. Proxy 17 will thus select the IP address of proxy 19 as the address used to forward the URL.

105. Alternatively, as described in Section X.A, ¶¶ 73, when proxy 17 receives from the client computer 11 a URL matching the criteria in text window 247, but not text window 253, including www.lucent.com, proxy 17 will “skip” the function of proxy 17, but will not “jump” over any server in the proxy chain because the URL does not match the “jump” criteria and will therefore select the IP address of proxy 19 so that the request passes “via the chained proxies 17, 19 and 21.”

EX1003, 4:29-31, 5:10-23, FIGs. 6-7. Proxy 17 thus will again select the IP address of proxy 19 as the address used to forward the URL.

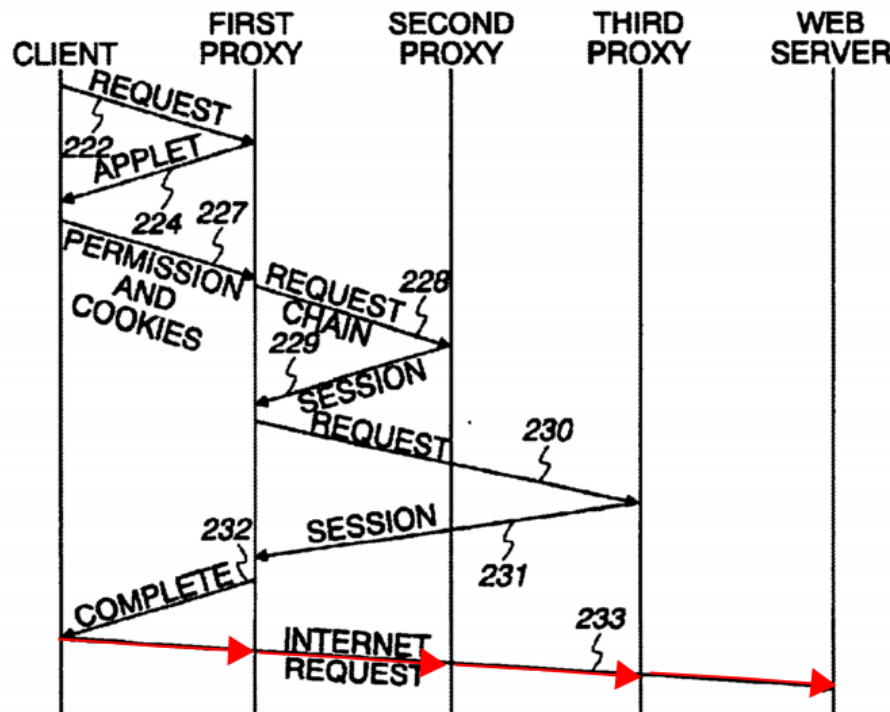
d. Limitation 1[c] sending, in response to the selecting, the first URL to the first web server using the selected IP address

106. In my opinion, Kocherlakota discloses or renders obvious this limitation. Kocherlakota teaches that the client access web servers via the chain of proxies.

(“Thereafter, the **client may access a web server** via the chain of proxies as represented by message 233.”) EX1003, 4:52-54.

107. As discussed for Limitation 1[b], proxy 17 (the claimed “first server”) selects the IP address of proxy 19 and, in response to the selecting, forwards the URL to proxy 19. EX1003, 4:29-31, 5:10-23, FIGs. 6-7. Proxy 17 forwards the URL to proxy 19 in order for the URL to be further forwarded by proxy 19 to proxy 21 and proxy 21 to the web server hosting the first URL (the claimed “first web server”) as shown in annotated FIG. 6 below.

Fig. 6



108. When proxy 17 sends a URL to an intermediary such as proxy 19, it uses the IP address of proxy 19 as a destination address. As this URL is eventually sent to the web server, the first server, proxy 17, is therefore using the selected IP address to send the first URL to the first web server. In addition, under the **PO Construction** of “source address,” when the intermediary proxy 19 forwards the received URL, the IP address associated with proxy 19 is used as the “source address.” Further, the selection of the IP address by proxy 19 is “in response to the receiving of the first URL” because the selection of the URL is based on analysis of the URL performed by proxy 17 when performing the “skipped” box 249 function.

e. Limitation 1[d]: receiving, in response to the sending of the first URL, the first content from the first web server.

109. In my opinion, Kocherlakota discloses or renders obvious this limitation. Kocherlakota teaches that proxies establish sessions to web servers and respond to internet data from those web servers.

(“Included in these servers are **proxies** which provide services to a user but which do so by establishing sessions with web servers and **responding to internet data from those web servers.**”) EX1003, 1:12-15.

110. As discussed for Limitations 1[b] and 1[c], proxy 17 forwards the first URL along the proxy chain to the web server corresponding to the first URL. A POSITA would understand that the function of a proxy, such as proxy 17 in the proxy chain, is both to send URLs to web servers, as well as receive responses from web servers and return them to the requesting client, otherwise the client would not be making use of accessing these web servers. Kocherlakota describes users “access[ing] the internet ‘through’ a proxy which provides value added to the **information accessed**” and proxy servers “responding to internet data from those web servers.” EX1003, 1:12-17. That is, client computer 11 obtains “access to web server 15 [] via the three web proxies 17, 19 and 21.” *Id.*, 3:9-11. By way of example, proxy 19 “provide[s] translations of identified files,” which requires that proxy 19 receives the files from the web server that are identified by the requested

URL and performs language translation on the received files. *Id.*, 1:28-31, 4:29-35 (“the language proxy 19 provides the French language features”).

111. Further, Kocherlakota describes web server 15 as a “data file provider[]” and “[a]fter the establishment of proxy sessions the client can surf the web through the established chain of proxy servers.” EX1003, 2:58-61, 2:30-32. POSITA would understand that the “web server” of Kocherlakota responds to web requests by providing a web page to the requesting device, as that is the purpose of web servers.

112. In the disclosed proxy chain, the web server corresponding to the first URL returns the web page corresponding to the first URL to proxy 21, proxy 21 forwards the web page to proxy 19, and proxy 19 forwards the web page to proxy 17. *Id.*, 2:58-61, 2:30-32, 4:29-35. Proxy 17 (the claimed “first server”) thus receives the web page corresponding to the first URL (the claimed “first content”) in response to the sending of the first URL.

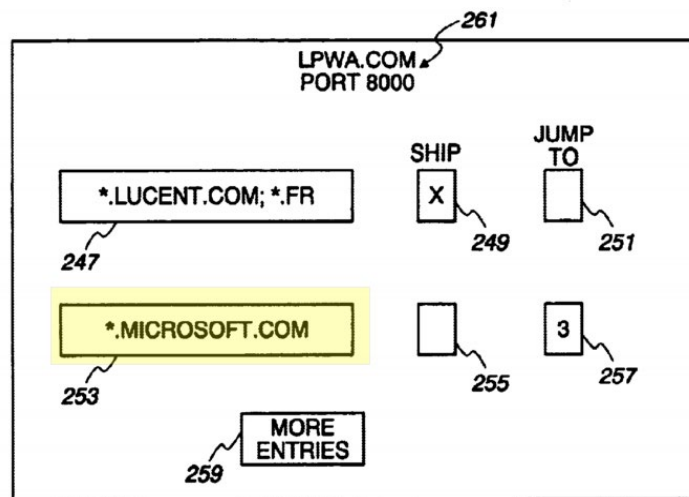
f. Limitation 1[e]: receiving, from the first client device, the second URL

113. In my opinion, Kocherlakota discloses or renders obvious this limitation. Kocherlakota teaches for example the first proxy receiving a different URL *.companyx.com which could be for example www.microsoft.com from the client.

(“Similarly, whenever a **URL of *.companyx.com is sent to the first proxy**, the first proxy will skip the second proxy and jump to the third proxy because the number 3 is entered into the jump to box 251. The advanced features allow the user to define which proxy servers are employed for predetermined URLs.”) EX1003, 5:21-26.

114. This second URL, for example `www.microsoft.com`, would match the criteria of text window 253 (“*.MICROSOFT.COM.”).

Fig. 7



g. Limitation 1[f]: selecting, in response to the receiving of the second URL from the first client device, an additional IP address from the group

115. In my opinion, Kocherlakota discloses or renders obvious this limitation. Kocherlakota teaches that Proxy 17 (the claimed “first server”) selects the IP address from the group of IP addresses for proxies 19 or 21 to route the URL through the proxy chain.

(“As shown in FIG. 7, when a URL matching *.lucent.com or *.fr is transmitted to the first proxy, the services of that proxy are to be skipped as defined by the “X” in box 249. Similarly, whenever a URL of *.companyx.com is sent to the first proxy, the **first proxy will skip the second proxy and jump to the third proxy** because the number 3 is entered into the jump to box 251. The advanced features allow the user to define which proxy servers are employed for predetermined URLs.”) EX1003, 5:18-26.

116. As discussed in Section X.A, ¶ 74 and for Limitation 1[e], upon receiving the second URL, proxy 17 (the claimed “first server”) selects the IP address of proxy 21 from the group of IP addresses to route the URL through the proxy chain. *Id.*, 5:10-23. Further, this selection is “in response to the receiving of the second URL” because the selection of the URL is based on analysis of the URL performed by proxy 17.

h. Limitation 1[g]: sending, in response to the selecting, the second URL to the second web server using the selected additional IP address

117. In my opinion, Kocherlakota discloses or renders obvious this limitation. As discussed for Limitation 1[f], proxy 17 selects the IP address of proxy 21 as the address used to forward the URL to proxy 21. EX1003, 5:21-26, FIGs. 6-7. Proxy 17 forwards the URL to proxy 21 in order for the URL to be further forwarded to the second web server hosting the second URL (the claimed “second web server”). *Id.*, 2:30-32; 4:52-54. When proxy 17 sends a URL to an intermediary, such as proxy 21, it uses the IP address of proxy 21. As this URL is eventually sent to the second web server, the first server, proxy 17, is therefore using the selected IP address to send the second URL to the second web server. A POSITA would understand that when proxy 17 sends the URL to proxy 21, the IP packets sent from proxy 17 to proxy 21 include the IP address of proxy 21 (the claimed “selected additional IP address”) as the destination IP address since these packets are being sent over the Internet. Proxy 17 therefore “uses” the selected additional IP address in sending the URL by using it as this destination address.

i. Limitation 1[h]: receiving, in response to the sending of the second URL, the second content from the second web server

118. In my opinion. Kocherlakota discloses or renders obvious this limitation. As discussed for Limitation 1[d], a POSITA would understand that the

web server will provide a web page corresponding to the received URL which will be forwarded back through the proxy chain to proxy 17. EX1003, 3:9-11, 1:28-31, 4:29-35, 2:58-61, 2:30-32. Thus, proxy 17 receives the web page corresponding to the second URL (the claimed “second content from the second web server”) in response to sending the second URL.

2. Claim 2: The method according to claim 1, wherein each of the IP addresses in the group is associated with a respective client device that is identified over the Internet using a respective IP address

119. In my opinion, Kocherlakota discloses or renders obvious this limitation. Proxy 19 and proxy 21 are client devices, as each is a device that communicates over the Internet and operate in the role of a client by establishing a connection down the proxy chain to make requests, as defined in RFC 2616, Section VII.A above. *See also* EX1005, 8/114 (proxy devices “act[s] as both a server and a client”). As described above in Limitation 1[p] and Section X.A, proxies 19 and 21 are connected to proxy 17 via sessions over the Internet.

(“FIG. 1 includes dotted line segments 12, 14 and 16 and solid line “loop’ segments **connecting each web proxy 17, 19 and 21 to the internet.**”)

EX1003, 3:3-5.

120. A POSITA would understand that in order to communicate over the Internet, each of the proxies 19 and 21 must be identified using their respective IP addresses (as the destination IP address) so the IP packet can be sent to these devices.

EX1015, 17/51; EX1016, 57/91. As described above in Limitation 1[p] and Section X.A, in order for proxy 17 to establish and maintain sessions with proxies 19 and 21, proxy 17 would also have and store the IP address corresponding to each of proxies 19 and 21.

3. Claim 3: The method according to claim 2, wherein the sending of the first URL to the first web server comprises sending, by the first server, the first URL to the client device addressed by the selected IP address

121. In my opinion, Kocherlakota discloses or renders obvious this limitation. As explained for Limitations 1[b] and 1[c], the process of proxy 17 sending the web request (containing the first URL, e.g., www.uspto.gov or www.lucent.com) to web server 15 includes proxy 17 (the claimed “first server”) sending the first URL to proxy 19 (the claimed “client device addressed by the selected IP address”) over the Internet.

(“FIG. 1 includes dotted line segments 12, 14 and 16 and solid line ‘loop’ segments **connecting each web proxy 17, 19 and 21 to the internet.**”)

EX1003, 3:3-5.

4. Claim 4: The method according to claim 3, wherein the sending of the first URL to the first web server further comprises sending, by the client device addressed by the selected IP address, the first URL to the first web server, and receiving, from the first web server, the first content

122. In my opinion, Kocherlakota discloses or renders obvious this limitation. As explained for Limitation 1[c], the process of proxy 17 sending the web

request (containing the first URL, e.g., www.uspto.gov or www.lucent.com) to web server 15 includes proxy 19 (the claimed “client device addressed by the selected IP address”) sending the first URL to proxy 21 for forwarding to the web server. As discussed for Limitation 1[c], Proxy 19 sending to an intermediary, proxy 21, for eventual sending to the web server meets the claim language “sending ... to the first web server” because this language includes sending to intermediaries for forwarding to the web server. As explained for Limitation 1[d], proxy 21 receives from the web server the web page corresponding to the first URL from web server 15 and then proxy 19 receives the web page from proxy 21, as these proxy servers are chained together.

(“When the **third proxy session is established, a session continues (step 125) between the client and a web server, e.g. 15, through proxy servers 17, 19 and 21.** The third proxy server establishes the session in a manner substantially similar to FIG. 5.”) EX1003, 4:23-28; *see also id.*, 2:58-61, 2:30-32, 3:3-5, 4:29-35.

5. Claim 5: The method according to claim 3, wherein the receiving of the first content from the first web server comprises receiving the first content from the client device addressed by the selected IP address.

123. In my opinion, Kocherlakota discloses or renders obvious this limitation. As explained in Limitation 1[d], proxy 17 (the claimed “first server)

receives the web page corresponding to the first URL (the claimed “first content”) from proxy 19 (the claimed “client device addressed by the selected IP address”).

(“When the third proxy session is established, **a session continues (step 125) between the client and a web server, e.g. 15, through proxy servers 17, 19 and 21.** The third proxy server establishes the session in a manner substantially similar to FIG. 5.”) EX1003, 4:23-28.

(“FIG. 1 includes dotted line segments 12, 14 and 16 and solid line ‘loop’ **segments connecting each web proxy 17, 19 and 21 to the internet.**”) *Id.*, 3:3-5.

6. Claim 6: The method according to claim 2, further comprising communicating, by the first server, with each of the client devices that are identified over the Internet using by the stored IP addresses

124. In my opinion, Kocherlakota discloses or renders obvious this limitation. Proxy 17 (the claimed “first server” establishes and maintains sessions, and thereby communicates, with each of proxies 19 and 21 (the claimed “each of the client devices”). EX1003, 4:43-54. As discussed in Limitation 1[p] and Section X.A, a POSITA would understand that the session setup and maintenance, as well as subsequent routing of URLs through the proxy chains to web servers, necessarily requires, or at a minimum renders obvious, proxy 17 storing a list the IP addresses of proxies 19 and 21. Communications by proxy 17 to each of proxies 19 and 21

use the stored IP address of proxies 19 and 21 as the “destination address” in accordance with IP protocols, as described in Claim 2.

7. Claim 7: The method according to claim 6, further comprising storing, by the first server, the IP addresses of each of the client devices in response to the communicating

125. In my opinion, Kocherlakota discloses or renders obvious this limitation. As discussed in Section X.A, Limitation 1[p] and Claim 6, a POSITA would understand that the session setup, necessarily requires, or at a minimum render obvious, proxy 17 storing a list the IP addresses of proxies 19 and 21. Where, for example, proxy 17 stores the IP addresses of proxies 19 and 21 to track an ongoing session, that storing is in response to the communicating with proxies 19 and 21 during session setup. *See* EX1003, 4:24-27.

8. Claim 10: The method according to claim 2, further comprising establishing, by the first server, a Transmission Control Protocol (TCP) connection with each of the client devices that are identified over the Internet using the IP addresses in the group

126. In my opinion, Kocherlakota discloses or renders obvious this limitation. As explained for Claim 6, proxy 17 communicates, with each of proxies 19 and 21 (the claimed “each of the client devices”) over the Internet. EX1003, 3:2-5. A POSITA would have knowledge of TCP and understand that one of the most common ways to communicate over the Internet is to use TCP.

(“As is known by those having ordinary skill in the art, TCPIP is a relatively low-level protocol, as opposed to HTTP, which is a high level protocol.”) EX1001, 17:22-24.

127. Further, as described in U.S. Patent 5,826,014, a cited reference to Kocherlakota, all Internet protocols are based on TCP and IP.

(All of the **Internet-compatible protocols**, however, **find some basis in the two original Internet protocols: TCP (Transmission Control Protocol) and IP (Internet Protocol).**) EX1018, 1:23-27.

128. Therefore in my opinion, it would have been obvious for a POSITA for to use the TCP protocol to communicate between the first server, proxy 17 to client devices, proxies 19 and 21.

129. A POSITA would also understand that the disclosed sending of URLs in Kocherlakoda indicates the communication is HTTP-based. EX1003, 3:21-4:35. A POSITA would understand that, as RFC 2616, which the '622 Patent recognizes “define[s]” “the HTTP protocol,” explains, “HTTP communication usually takes place over TCP/IP connections.” See EX1001, 16:21-22, 17:20-26; EX1005, 11/114. A POSITA would also understand that communicating over TCP requires establishing, by the communicating devices, a TCP session. See EX1016, 16-18/91. Thus, a POSITA would understand that Kocherlakota’s disclosure of proxy 17 communicating with each of proxies 19 and 21 discloses or renders obvious proxy

17 communicating using TCP/IP, including establishing a TCP connection with each of proxies 19 and 21.

9. Claim 14: The method according to claim 1, for use with a criterion stored in the first server, wherein the selecting is according to, or based on, the criterion

130. In my opinion, Kocherlakota discloses or renders obvious this limitation. As discussed for Limitations 1[b] and 1[f], proxy 17 performs each of the selecting steps by applying the criteria shown in FIG. 7 (i.e., applying “skip” and “jump” when a URL matches the criteria in a text window) as well as the default routing defined in FIG. 2 (each individually or collectively the claimed “criterion”). EX1003, 5:10-26. After the first proxy server 17 receives the applet and relevant session information, the first proxy server uses this information to route the URL. Accordingly, the criterion information identified in FIGs. 2 and 7, must be stored in proxy server 17 to be used in routing URLs. *Id.*, 3:61-67.

10. Claim 16: The method according to claim 14, wherein the criterion is based on, or comprises, a geographic location of the client device addressed by the selected IP address

131. In my opinion, Kocherlakota discloses or renders obvious this limitation. Kocherlakota discloses “French language web proxy 19” provides “language service[s],” which, as discussed for Limitation 1[b], may be address by the selected IP address. EX1003, 2:65-67. A POSITA would understand the French language services are, or would be obvious to be, associated with a geographic

location—France. Further, Kocherlakota discloses matching criteria “*.fr,” which a POSITA would understand is the top-level domain for France—a geographic location. EX1003, FIG. 7.

132. In addition, Kocherlakota discloses “an efficiency proxy” that “may contain a local cache for storing frequently accessed files.” EX1003, 1:31-36. It would have been obvious to have such an efficiency proxy dedicated to a geographic location, such as a city or region, which would have a unique set of “frequently accessed files,” and to use criteria for that geographic area to select that efficiency proxy to reduce the amount of time spent retrieving data. As Kocherlakota, acknowledges, users value protections “against delays of internet usage...” *Id.*, 1:32-33.

11. Claim 17: The method according to claim 14, wherein the criterion is based on, or comprises, a response time when communicating.

133. In my opinion, Kocherlakota discloses or renders obvious this limitation. Each of the criteria in FIG. 7 is based on a response time because they are paired with actions—“skip[ping]” “the services of a proxy” or wholly “skip[ping]” a proxy—that impact the response time to return content to client computer 11. Therefore, the selection will impact the response time, and therefor comprises a response time when communication. EX1003, 4:55-5:26.

134. Moreover, measuring response time for servers was well known, and in my opinion it would have been obvious for a POSITA to base the selection of a proxy on response time as it would improve the customer's experience. As Kocherlakota acknowledges, users value protections "against delays of internet usage sometimes referred to as the world wide wait." *Id.*, 1:32-33; *see also id.*, 3:1-3 ("...the client would like to reduce the amount of time spent retrieving data so the services of a wait limiting proxy 21 are desired.).

12. Claim 20: The method according to claim 1, further comprising sending the received first content to the first client device.

135. In my opinion, Kocherlakota discloses or renders obvious this limitation. Client computer 11 obtains "access to web server 15 [] via the three web proxies 17, 19 and 21." EX1003, 3:9-11. As discussed for Limitation 1[d], the function of a proxy such as proxy 17 in the proxy chain is both to send URLs to web servers, as well as receive responses from web servers and return them to the requesting client, otherwise the client would never see the web pages accessed. As explained for Limitation 1[d], proxy 17 (the claimed "first server") receives the web page corresponding to the first URL (the claimed "first content"). In accordance with its function as a proxy and providing client computer 11 "access to web server 15," proxy 17 sends the received first content to client computer 11 (the claimed "first client device").

13. Claim 21: The method according to claim 20, further comprising sending the received second content to the first client device

136. In my opinion, Kocherlakota discloses or renders obvious this limitation. As discussed for Limitation 1[h], proxy 17 receives the web page corresponding to the second URL (the claimed “second content”) or the client would never see the web page they were trying to access. As discussed for Claim 20, in accordance with its function as a proxy and providing client computer 11 “access to web server 15,” proxy 17 sends the received second content to client computer 11 (the claimed “first client device”). EX1003, 3:9-11.

14. Claim 22: The method according to claim 1, wherein the first client device is addressed over the Internet using a first Internet Protocol (IP) address, and the method further comprising storing, in the first server, the first IP address.

137. In my opinion, Kocherlakota discloses or renders obvious this limitation. As shown in FIG. 1, client computer 11 (the claimed “first client device”) and proxy 17 (the claimed “first server”) communicate over the Internet. EX1003, FIG. 1, 3:3-8. A POSITA would understand that client computer 11 is addressed over the Internet using an IP address (the claimed “first IP address”) because a POSITA would understand that devices on the Internet are addressed by IP address. EX1015, 17/51; EX1016, 57/91. Further, as described in Section X.A, ¶¶ 77-78, a POSITA would have also understood proxy 17 stores the IP address of client computer 11 to establish and maintain sessions. EX1003, 3:21-23.

15. Claim 23: The method according to claim 1, wherein the first server is a Transmission Control Protocol/Internet Protocol (TCP/IP) server that communicates over the Internet with client devices based on, according to, or using, TCP/IP protocol or connection.

138. In my opinion, Kocherlakota discloses or renders obvious this limitation. As discussed in Section X.A and Limitation 1[p], proxy 17 (the claimed “first server”) is a server and, as discussed for Claim 10, Kocherlakota discloses or renders obvious proxy 17 communicating with proxies 19 and 21 (the claimed “client devices”) over the Internet using TCP/IP.

16. Claim 24: The method according to claim 1, wherein the first server communicates over the Internet based on, or according to, one out of UDP, DNS, TCP, FTP, POP#, SMTP, or SQL standards.

139. In my opinion, Kocherlakota discloses or renders obvious this limitation for at least the reasons discussed in Claim 23.

17. Claim 26: The method according to claim 1, for use with a second client device, the method further comprising, by the first server: receiving a message from the second client device; and responsive to the receiving of the message from the second client device, adding the IP address of the second device to the group of IP addresses

140. In my opinion, Kocherlakota discloses or renders obvious this limitation. Proxy 19 (the claimed second client device) sends a message back to proxy 17 (the claimed first server) to signify the establishment of a session.

(A request is sent 228 to the second proxy which authenticates it and **returns a message 229 to the first proxy signifying the session establishment.**)

EX1003, 4:46-48; *see also id.*, 4:2-4, FIGs. 4, 6.

141. As discussed for Claim 2, proxy 19 (the claimed “second client device”) is a client device. After establishing sessions between the client, the “first proxy server [17] and second proxy server [19], the client can access the internet by sending URLs through the chained first and second proxies.” *Id.*, 2:4-7. As explained in Section X.A and Limitation 1[p], proxy 17 stores the IP address of proxy 19 to establish and maintain a session. Accordingly, proxy 17 adds the IP address of the second device “proxy 19” to the group of IP addresses responsive to receipt of message 229.

18. Claim 27: The method according to claim 1, wherein the sending of the first URL to the first web server comprises using the selected IP address as a source address.

142. In my opinion, Kocherlakota discloses or renders obvious this limitation. As discussed for Limitation 1[c], under the **PO Construction** of “source address,” when by proxy 19 further forwards towards the web server, the IP address associated with proxy 19 is used as the “source address.”

143. Kocherlakota also discloses placing the number 3 in “jump to box” such that “the first proxy will skip the second proxy and jump to the third proxy.” EX1003, 5:21-23. This functionality “allow[s] the user to define which proxy

servers are employed for predetermined URLs.” *Id.*, 5:24-26. In order to achieve this goal of enabling “the user to define which proxy servers are employed for predetermined URLs,” it would have been obvious to enable the user to specify web server in a “jump to box,” thus skipping all remaining proxies. Such functionality would improve the customer’s experience for selected URL by reducing response time. *See* EX1003, 1:32-33 (disclosing that users value protections “against delays of internet usage sometimes referred to as the world wide wait”). In such a case, the group of IP addresses stored by proxy 17 would also include the IP address of the web server—which would need to be stored to maintain sessions just like the IP addresses of proxies 19 and 21 as discussed in Section X.A—and proxy 17 would select the IP address of the web server when the received URL matched criteria specified in the text box corresponding to the “jump to” box.

19. Claim 28: The method according to claim 1, further comprising sending, by the first server, the selected IP address in response to the selecting.

144. In my opinion, Kocherlakota discloses or renders obvious this limitation. As explained for Limitation 1[c], proxy 17 sends the URL to proxy 19 in response to the selecting. As explained for Claim 6, when proxy 17 sends IP packets to proxy 19, it uses the IP address of proxy 19 (the claimed “selected IP address”) as the “destination address.” The “destination address” is part of the IP header and is thus sent with the IP packet. *See* EX1015, 17/51; EX1016, 57/91.

20. Claim 29: The method according to claim 1, wherein the first client device is identified by a first Internet Protocol (IP) address, Media Access Control (MAC) address, or a hostname.

145. In my opinion, Kocherlakota discloses or renders obvious this limitation. As explained for Claim 22, client computer 11 (the claimed “first client device”) is identified by an IP address (the claimed “first IP address”). *See* EX1015, 17/51; EX1016, 57/91.

21. Claim 30: The method according to claim 1, further comprising storing, operating, or using, by the first server, a server operating system.

146. In my opinion, Kocherlakota discloses or renders obvious this limitation. First, as the '622 Patent acknowledges, (i) an operating system of a computer was known, and (ii) an internet browser was known, and other “program[s] that would be used to request data that is stored on a Web server” were known. EX1001, 6:31-47. Further, as discussed in Section X.A, a POSITA would know that a proxy server, such as proxy 17 (the claimed “first server”), makes use of an operating system as they are required to manage, store and execute programs that allow hardware to establish connections with web servers. This is particularly true for servers, such as proxy 17, that communicate over the internet with web servers through HTTP and TCP/IP protocols. *See* EX1005, 71/114 (describing the use of “HTTP servers” as using “UNIX, Microsoft Windows, and other operating

systems”); *see also* EX1016, 14/191 (stating that “TCP is assumed to be a module in an operating system”).

22. Claim 31: The method according to claim 1, for use with a software application that includes computer instructions that, when executed by a computer processor, cause the processor to perform the steps of the claim 1.

147. In my opinion, Kocherlakota discloses or renders obvious this limitation. As explained for Claim 30, a POSITA would understand that, as is the nature of computing devices, proxy 17 would including a processor and perform those steps by executing a software application that includes computer instructions causing the processor to perform the steps.

23. Claim 32: The method according to claim 1, wherein the first web server comprises a web server that is a Hypertext Transfer Protocol (HTTP) server responding to HTTP requests and addressed in the Internet using a web server Internet Protocol (IP) address

148. In my opinion, Kocherlakota discloses or renders obvious this limitation. Kocherlakota describes “web server 15” (the claimed “first web server”) as “representative of any of the well known data file providers and, in fact, represents the universe of addressable web servers.” EX1003, 2:58-61. This would include an HTTP server as HTTP servers were well known providers of files including documents and database information. *See* EX1019, 2:43-53 (describing a server as comprising “standard web server functionality (e.g., HTTP server)...[that] determine[s] the object (e.g., documents or databases) specified by the URL,

retrieves that object, translates that object to HTML format and sends the HTML downloaded object to the client side browser for display.”); *see also* EX1005, 94/114 (describing an HTTP as translating “HTTP URIs directly into file system calls...”).

149. Further, a POSITA would understand that a web server receiving HTTP web requests containing URLs would be a responding HTTP server, addressed on the Internet using an IP address (e.g., the IP address of web server 15). Specifically, as discussed in VII.A, it was known or at least obvious to use HTTP in conjunction with TCP/IP, in which case the web server 15 would be addressed on the Internet using its IP address. EX1005, 11/114; *see also* EX1001, 17:17-20 (recognizing DNS).

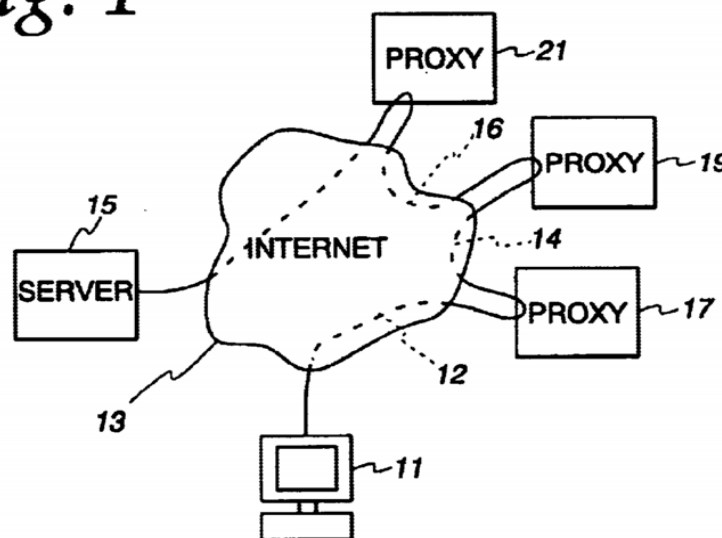
B. Ground 2 – Kocherlakota in View of RFC 1122 Renders Obvious Claims 8-9, 11-13

150. In my opinion, Kocherlakota in view of RFC 1122 renders obvious claims 8-9, 11-13.

1. Motivation to combine

151. A POSITA would have been motivated to use the TCP keep-alive functionality of RFC 1122, as discussed in Section X.B above, when maintaining TCP sessions as disclosed by Kocherlakota for Claim 10. Both references cover connecting Internet hosts over the Internet. RFC 1122 describes an Internet host as “A host computer, or simply "host," is the ultimate consumer of communication services.” EX1006, 6/116. Kocherlakota describes methods and apparatus for establishing internet communication from a user to a server through a plurality of proxy servers. [Abstract] FIG. 1 demonstrates that the web server 15, client 11, and proxies 17, 19 and 21 are the consumer, or terminator of Internet communications services described in RFC 1122.

Fig. 1



152. A POSITA would have recognized the benefits of Kocherlakota's proxy servers exchanging TCP keep-alives with each other. One benefit, TCP keep-alives help detect when "a client crashes or aborts a connection during a network failure" and thus prevent server applications from "hang[ing] indefinitely and consum[ing] resources unnecessarily." EX1006, 102/116. For example, following the establishment of sessions between proxy 17 and the client computer 11, proxy 19 and/or proxy 21, one of client computer 11, proxy 19, or proxy 21 could crash. This could lead to the situation where proxy server 17 sends Internet traffic to a proxy that no longer operational. This could lead to lost messages and unnecessarily expend resources keeping the "dead" TCP connection open. Another benefit a POSITA would have known of is that TCP keep-alives could also prevent periods of inactivity between client devices from causing the TCP connection between them to terminate. Which again could result in lost messages.

153. RFC 1122 does specify some potential disadvantages of TCP keep-alives, including additional bandwidth consumption and "cost money for an Internet path that charges for packets." EX1006, 102/116. However, a POSITA would have recognized that these disadvantages are *de minimis* because "[a]n implementation SHOULD send a keep-alive segment with no data" (EX1006, 102/116) and Internet service providers most frequently charge a flat rate for bandwidth usage rather than

per packet. As a result, these potential disadvantages are outweighed by the benefits listed above in a system such as the interconnected proxy servers of Kocherlakota.

2. Modification of Kocherlakota in view of RFC 1122

154. A POSITA would have modified Kocherlakota so that the sessions between proxy 17 and client computer 11, proxy 19 and/or proxy 21, would periodically communicate by exchanging TCP keep-alive messages with each other over established TCP connections. A "keep-alive" mechanism was a well-known technique, which periodically probes the other end of a connection when the connection is otherwise idle, even when there is no data to be sent. EX1006, 102/116. In the proxy chain comprising a client computer 11 -> proxy 17 -> proxy 19 or the proxy chain comprising a computer 11 -> proxy 17 -> proxy 21 proxy, the proxy 17 would periodically send client computer 11 and proxies 19 and/or 21 keep-alive messages over the TCP connections between them. Further, in accordance with RFC 1122, the proxy 17 would wait for an "acknowledgment" from proxies 19 and/or 21, confirming that the connection is still live.

155. Such a modification would be simple for a POSITA, as all that is required is to send a probe segment designed to elicit a response from the peer TCP periodically. EX1006, 102/116.

- 3. Claim 8: The method according to claim 6, further comprising receiving a ‘keep alive’ message, by the first server, from each of the client devices that are identified over the Internet using by the stored IP addresses.**

156. In my opinion, Kocherlakota-RFC 1122 renders obvious this limitation. As described above in Claim 6, Kocherlakota discloses how each of the client devices are identified over the Internet using by the stored IP addresses. As described above, the combination of RFC1122 would make it obvious for a POSITA to use TCP keep-alives to maintain the sessions between proxy 17 and proxies 19, and 21.

- 4. Claim 9: The method according to claim 2, wherein each of the IP addresses in the group is associated with a respective client device that is identified over the Internet using a respective IP address and is currently online**

157. In my opinion, Kocherlakota-RFC 1122 renders obvious this limitation. As described above in Claim 2, Kocherlakota discloses how the client devices are identified over the Internet using a respective IP address. The addition of TCP keep-alives from RFC1122 would allow a POSITA to identify if a TCP connection were alive, and if it was alive, A POSITA would know the client device was online.

- 5. Claim 11: The method according to claim 1, further comprising by the first server: sending, a ‘keep alive’ message to each of the client devices that are identified over the Internet using by the stored IP addresses; and waiting for a response to the ‘keep alive’ message from each of the client devices.**

158. In my opinion, Kocherlakota-RFC 1122 renders obvious this limitation. This limitation is just a recitation of the well-known algorithm for keep alives. As

described above, as all that is required is for the first server to send a probe segment designed to elicit a response from the peer TCP periodically as described in RFC 1222. EX1006, 102/116.

- 6. Claim 12: The method according to claim 11, further comprising responsive to not receiving, by the first server, a response to the ‘keep alive’ message from a client device, removing the IP address of the non-responsive third client device from group of IP addresses.**

159. In my opinion, Kocherlakota-RFC 1122 renders obvious this limitation. As discussed above in Claim 9, it would have been obvious for a POSITA to identify if a client device were online or not. If the device was offline, it would have been obvious for a POSITA remove the IP address of a non-responsive client device from the list of IP addresses of devices under active session in order to save system resources and prevent message being sent to a ‘dead’ device.

- 7. Claim 13: The method according to claim 11, wherein the sending of the ‘keep alive’ message comprises periodically sending by the first server the ‘keep alive’ message to at least part of the client devices.**

160. In my opinion, Kocherlakota-RFC 1122 renders obvious this limitation. This limitation is just a recitation of the well-known algorithm for keep alives. As described above, as all that is required is for the first server to send a probe segment designed to elicit a response from the peer TCP **periodically** as described in RFC 1222. EX1006, 102/116.

C. Ground 3 – Cohen Renders Obvious Claims 1-14, 17, 20-24, 26-32

1. Claim 1

- a. Limitation 1[p]: A method for fetching, by a first client device, a first content that comprises a web-page, an audio, or a video content, and is identified by a first Uniform Resource Locator (URL) and stored in a first web server, for fetching, by the first client device, a second content that comprises a web-page, an audio, or a video content, and is identified by a second URL and stored in a second web server, for use with a first server that stores a group of IP addresses, the method by the first server comprising.**

161. In my opinion, Cohen discloses or renders obvious this limitation. Cohen discloses a method by for fetching by a client 101-1 (the claimed “first client device”) a web page identified by a first URL associated with an origin server (containing the claimed “first content”) through proxy redirector 104 as well as a different web page identified by a second URL associated with a different origin server (containing the claimed “second content”) through proxy redirector 104.

162. Cohen discloses proxy redirector 104 which intercepts a web request from a “client 101-1” seeking content from a target web server and establishes a TCP connection between the client and the selected proxy.

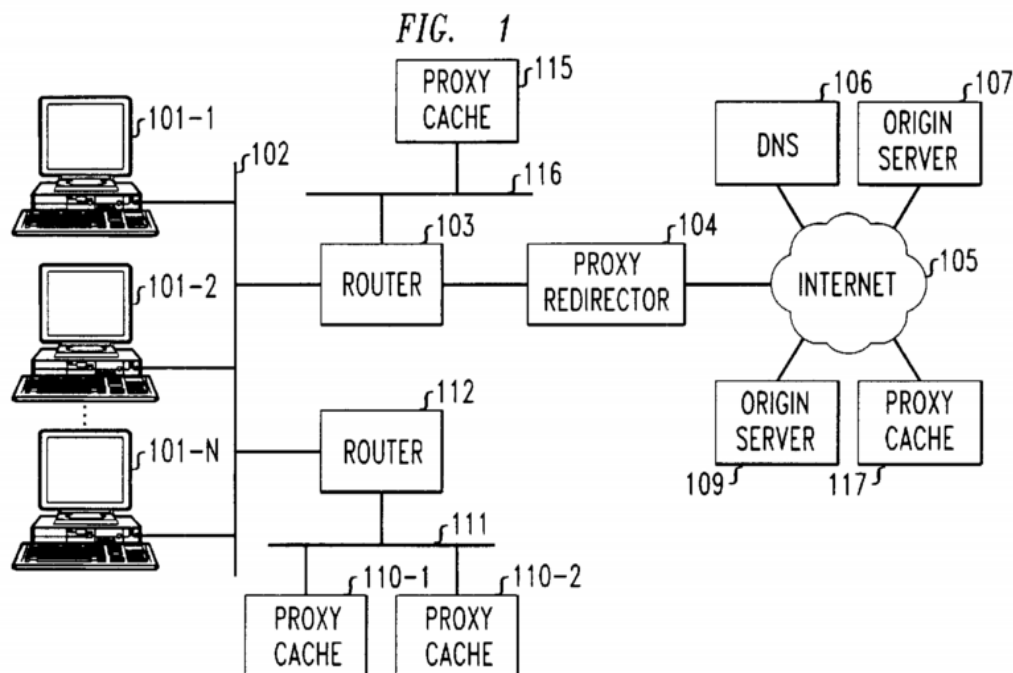
(“In accordance with the present invention, once the IP address of the origin server corresponding to the logical URL name is determined through the DNS

look-up, **proxy redirector 104**, rather than establishing a TCP connection to the origin server at the determined IP address, **transparently establishes a TCP connection between the client and a proxy.**') EX1004, 7:12-19.

163. Proxy selects one of the available proxy caches to which to forward client requests based on a metric such as least-loaded or round-robin, [or] based on IP header information such as the origin server IP address.

(“**Proxy redirector 104 selects one of the available proxy caches** to which to forward client requests based on a metric Such as least-loaded or round-robin, based on IP header information such as the origin server IP address.”)

Id., 43-47. See FIG.1 below.



164. Specifically, the “proxy redirector 104” intercepts a web request from a “client 101-1” seeking content from a target web server and “selects one of the available proxy caches [e.g. 110-1, 110-2, 115, and 117] to which to forward client requests based on a metric such as least-loaded or round-robin, [or] based on IP header information such as the origin server IP address.” *Id.*, 7:36-48; *see also id.*, 2:15-20.

165. Cohen teaches that after the TCP connection is established, the client sends “one or more packets to the origin server [via the proxy redirector 104], which packets include a GET request. The GET request includes a complete URL, which identifies to that server the specific object within the origin server site that the client wants a copy of.” *Id.*, 9:19-22.

(“After the TCP connection is established between client 101-1 and proxy cache 110-1, **client 101-1 sends one or more packets containing a GET request** addressed to the origin server. Such packets are thus “captured’ by proxy redirector 104 and redirected to proxy cache 110-1. As previously discussed, the **GET request sent by the client contains only the complete URL** sent by the client browser 25 which in itself provides insufficient information for the proxy cache to determine whether it has the requested object and, if not, to forward it to the origin server which does.”) *Id.*, 9:19-28.

166. A POSITA would have understood and/or it would have been obvious for the client 101-1 to seek additional content from a second target web server with a different URL, as a client device which seeks to access only a single web server on the Internet makes sense in the context of Internet browsing.

167. Client 101-1 meets the construction of “client device” because it is a device that communicates over a network and it is operating in the role of a client by making requests for objects. *Id.*, 9:19-21. (“client 101-1 sends one or more packets containing a GET request addressed to the origin server.”).

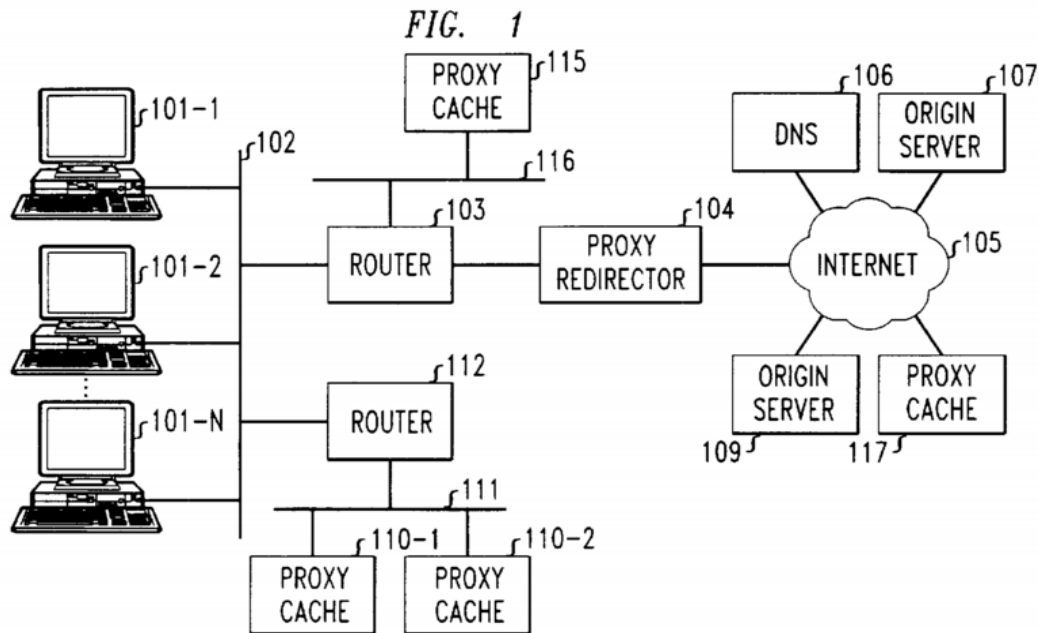
168. Proxy redirector 104 meets the construction of “first server” because it is a device operating in the role of a server by receiving client 101-1’s web requests and sending the responses back to client 101-1 and because it is not the same physical device as client 101-1 (the claimed “first client device”). (“Responsive packets from the proxy cache are sent to proxy redirector 104 where they are redirected to client 101-1.”) *Id.*, 8:57-59.

169. As discussed in Section X.C above, in order to select one of the many available proxy caches, proxy redirector 104 must store a list of the IP addresses associated with each proxy cache (the claimed “list of IP addresses”).

(“**Proxy redirector 104 selects one of the available proxy caches** to which to forward client requests based on a metric such as least-loaded or round-

robin, based on IP header information such as the origin server IP address.”)

Id., 7:43-47; *see* Fig. 1 below.



b. Limitation 1[a]: receiving, from the first client device, the first URL

170. In my opinion, Cohen discloses this limitation. Cohen discloses that the client sends “one or more packets to the origin server [via the proxy redirector 104], which packets include a GET request. The GET request includes a complete URL, which identifies to that server the specific object within the origin server site that the client wants a copy of.” EX1004, 2:15-20.

171. As shown in Table 1 (annotated below), the proxy redirector 104 (the claimed “first server”) receives the GET request from client 101-1 (the claimed “first client device”) with the included complete URL “/a/ya/yahoomail/promo1.gif HTTP/1.0” (the claimed “first URL”) designated as the arriving packet. EX1004, 9:19-23; Table 1; see also *Id.*, 2:15-20.

TABLE 1

Arriving packet:	
---	beginning of packet header dump <---
---	IP header: version=4 hdr_len=5 TOS=0 pkt_len=346 id=60276 frag_off=4000H TTL=64 protocol=6 cksum=1792H saddr=135.104.25.243 daddr=204.71.200.244
---	TCP header: sport=1273 dport=80 seq=2189084427 ack_seq=3266449517 tcp_hdr_len=5 flags=ACK PSH res1=0H res2=0H window=31856 cksum=162H urgent=0
---	beginning of packet data dump <---
	GET /a/ya/yahoomail/promo1.gif HTTP/1.0
	Referer: http://www.yahoo.com/
	Connection: Keep-Alive
	User-Agent: Mozilla/4.05 [en] (X11; U; Linux 2.1.103 i686)
	Host: us.yimg.com
	Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg image/png
	Accept-Language: en
	Accept-Charset: iso-8859-1, *,utf 8
	Modified to:
---	beginning of packet header dump <---
---	IP header: version=4 hdr_len=5 TOS=0 pkt_len=367 id=60276 frag_off=4000H TTL=64 protocol=6 cksum=1792H saddr=135.104.25.245 daddr=135.104.25.31
---	TCP header: sport=5000 dport=7000 seq=2189084427 ack_seq=3266449517 tcp_hdr_len=5 flags=ACK PSH res1=0H res2=0H window=31856 cksum=162H urgent=0
---	beginning of packet data dump <---
	GET http://204.71.200.244/a/ya/yahoomail/promo1.gif HTTP/1.0
	Referer: http://www.yahoo.com/
	Connection: Keep-Alive
	User-Agent: Mozilla/4.05 [en] (X11; U; Linux 2.1.103 i686)
	Host: us.yimg.com
	Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg image/png
	Accept-Language: en
	Accept-Charset: iso-8859-1, *,utf 8

c. Limitation 1[b]: selecting, in response to the receiving of the first URL from the first client device, an IP address from the group

172. In my opinion, Cohen discloses this limitation. As shown in Table 1 (annotated below), upon receiving the URL, proxy redirector 104 (the claimed “first server”) selects the IP address “daddr=135.104.25.31” of a proxy cache 110-1 from the group of IP addresses associated with at least two or more proxies (i.e. proxies 110-1, 110-2, 115, and/or 117) to forward the URL to the selected proxy. EX1004, 11:12-15.

TABLE 1

Arriving packet:	
---	beginning of packet header dump <---
---	IP header: version=4 hdr_len=5 TOS=0 pkt_len=346 id=60276 frag_off=4000H TTL=64 protocol=6 cksum=1792H saddr=135.104.25.243 daddr=204.71.200.244
---	TCP header: sport=1273 dport=80 seq=2189084427 ack_seq=3266449517 tcp_hdr_len=5 flags=ACK PSH res1=0H res2=0H window=31856 cksum=162H urgent=0
---	beginning of packet data dump <---
	GET /a/ya/yahoomail/promo1.gif HTTP/1.0 Referer: http://www.yahoo.com/ Connection: Keep-Alive User-Agent: Mozilla/4.05 [en] (X11; U; Linux 2.1.103 i686) Host: us.yimg.com Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg image/png Accept-Language: en Accept-Charset: iso-8859-1, *,utf 8 Modified to:
---	beginning of packet header dump <---
---	IP header: version=4 hdr_len=5 TOS=0 pkt_len=367 id=60276 frag_off=4000H TTL=64 protocol=6 cksum=1792H saddr=135.104.25.245 daddr=135.104.25.31
---	TCP header: sport=5000 dport=7000 seq=2189084427 ack_seq=3266449517 tcp_hdr_len=5 flags=ACK PSH res1=0H res2=0H window=31856 cksum=162H urgent=0
---	beginning of packet data dump <---
	GET http://204.71.200.244/a/ya/yahoomail/promo1.gif HTTP/1.0 Referer: http://www.yahoo.com/ Connection: Keep-Alive User-Agent: Mozilla/4.05 [en] (X11; U; Linux 2.1.103 i686) Host: us.yimg.com Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg image/png Accept-Language: en Accept-Charset: iso-8859-1, *,utf 8

173. This selection is “in response to the receiving of the first URL” because the selection of the URL can be “based on IP header information such as the origin server IP address. *Id.*, 7:43-48.

d. Limitation 1[c] sending, in response to the selecting, the first URL to the first web server using the selected IP address

174. In my opinion, Cohen discloses this limitation. As discussed for Limitation 1[b], the proxy redirector 104 selects the IP address of proxy cache 110-1 and, in response to the selecting, forwards the URL to proxy cache 110-1. EX1004, 7:36-48; *see also id.*, 11:12-15 (“As can be noted in the modified packet, the packet is redirected to a proxy cache 110-1 at IP address 135.104.25.31 port 7000 by changing the daddr and dport header information.”). Further, if the proxy cache to which the request is directed does not contain the requested object, “a separate TCP connection is established **between the proxy cache and the origin server** [e.g. origin server 107 or 109] **to obtain a copy of the requested object.**” *Id.*, 7:27-31.

175. A POSITA would understand that when proxy redirector sends the URL to the first web server through to proxy cache 110-1, as an intermediary, proxy redirector uses the IP address associated with proxy cache 110-1 (the claimed “selected IP address”) as the destination IP address in the IP packets. Further, under the **PO Construction** of “source address,” when by proxy cache 110-1 forwards towards the web server, the IP address associated with proxy cache 110-1 is used as

the “source address.” Section X.C above. “If the proxy cache to which the request is directed does not contain the requested object, a separate TCP connection is established between the proxy cache and the origin server to obtain a copy of the requested object.” *Id.*, 7:27-35.

e. Limitation 1[d]: receiving, in response to the sending of the first URL, the first content from the first web server;

176. In my opinion, Cohen discloses this limitation. As discussed for Limitations 1[b] and 1[c], proxy redirector 104 forwards the first URL to proxy cache 110-1, which establishes a TCP connection to the origin server to obtain the requested object (the claimed “first content”) if it does not have the stored content. A POSITA would understand that the function of a proxy such as proxy redirector 104 is both to forward URLs to web servers, as well as receive responses from web servers and return them to the requesting client. If not, then the client is not receiving the object that they have requested.

(“The GET request includes a complete URL, which identifies to that server the **specific object within the origin server site that the client wants a copy of.**”) EX1004, 2:17-19.

177. In addition, Cohen discloses that “[P]ackets from a client 101-1 are transparently directed by proxy redirector 104 to a proxy cache. Responsive packets from the proxy cache are sent to proxy redirector 104 where they are redirected to

client 101-1.” *Id.*, 8:55-58; *see also Id.*, 6:39-46, 10:23-25, 12:18-20. Cohen further explains that the proxy cache returns the “requested objects” (i.e. the claim “first content”) to the address from which a request originated. *Id.*, 16:28-41.

f. Limitation 1[e]: receiving, from the first client device, the second URL

178. In my opinion, Cohen discloses this limitation. Cohen discloses that the “invention relates to... a network for transparently intercepting **client web requests** and redirecting them to proxy caches.” EX1004, 1:6-10. Accordingly, it would have been obvious to a POSITA based on the disclosures and teachings of Cohen, as discussed in Limitation 1[a], for client 101-1(the claimed “first client”) to send a second GET request that includes a second complete URL (the claimed “second URL”) to the proxy redirector 104. *Id.*, 9:19-23; Table 1; *see also id.*, 2:15-20.

g. Limitation 1[f]: selecting, in response to the receiving of the second URL from the first client device, an additional IP address from the group

179. In my opinion, Cohen discloses this limitation. As discussed in Limitation 1[b], upon receiving the second URL, it would have been obvious to a POSITA that proxy redirector 104 (the claimed “first server”) would select an additional IP address corresponding to a different proxy cache (e.g. 110-2) from the group of IP addresses associated with the proxies (i.e. proxies 110-1, 110-2, 115,

and/or 117) to forward the URL to the selected proxy. EX1004, 7:43-48; 11:12-15. A POSITA would understand that each of the proxy caches 115, 110-1, 110-2 and 117 would have different IP addresses.

h. Limitation 1[g]: sending, in response to the selecting, the second URL to the second web server using the selected additional IP address

180. In my opinion, Cohen discloses this limitation. As discussed in Limitation 1[c], it would have been obvious to a POSITA that proxy redirector 104 forwards the second URL to a different proxy cache (e.g. 110-2) using the selected IP address of proxy cache 110-2 as the destination IP address. EX1004, 7:43-48; 11:12-15.

i. Limitation 1[h]: receiving, in response to the sending of the second URL, the second content from the second web server

181. In my opinion, Cohen discloses this limitation. As discussed for Limitation 1[d], a POSITA would understand that a second web server will provide a web page corresponding to the second URL, which will be forwarded back to the proxy redirector 104. EX1004, 8:55-58; *see also id.*, 6:39-46, 10:23-25, 12:18-20.

2. Claim 2: The method according to claim 1, wherein each of the IP addresses in the group is associated with a respective client device that is identified over the Internet using a respective IP address.

182. In my opinion, Cohen discloses or renders obvious this limitation. Proxies 110-1, 110-2, 115, and/or 117 each meet the construction of “client device”

because each is a device that communicates over the Internet and operate in the role of a client by establishing a connection between the origin server and the proxy redirector 104. See Limitation 1[b]; *see also* EX1005, 8/114 (proxy devices “act[s] as both a server and a client”). As discussed in Section X.C above, to be selectable by the proxy redirector as Cohen describes, a POSITA would have understood that each of the proxies 110-1, 110-2, 115, and/or 117 are identified using a respective IP address. EX1015, 17/51; EX1016, 57/91.

3. Claim 3: The method according to claim 2, wherein the sending of the first URL to the first web server comprises sending, by the first server, the first URL to the client device addressed by the selected IP address.

183. In my opinion, Cohen discloses or renders obvious this limitation. As explained in Section X.C and Limitations 1[b] and 1[c], the process of proxy redirector 104 sending the GET request (containing the first URL, e.g. “/a/ya/yahoomail/promo1.gif HTTP/1.0”) to the origin server (e.g. origin server 107 or 109) includes proxy redirector 104 (the claimed “first server”) sending the first URL to proxy cache 110-1 (the claimed “client device addressed by the selected IP address”).

4. Claim 4: The method according to claim 3, wherein the sending of the first URL to the first web server further comprises sending, by the client device

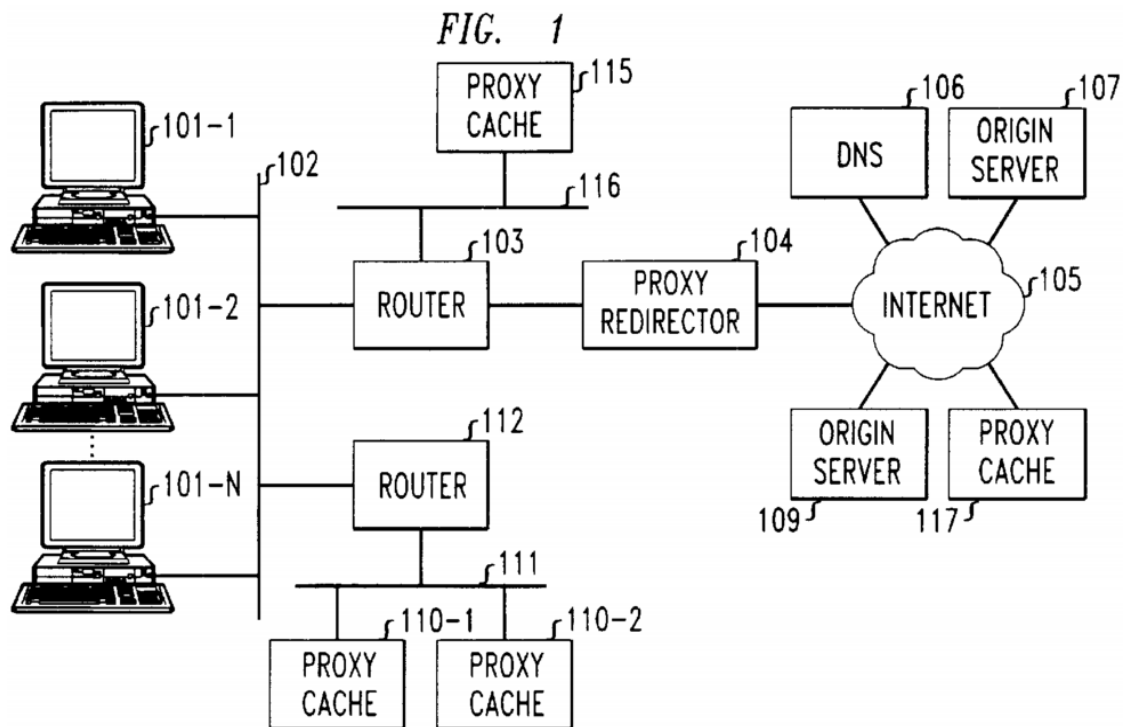
addressed by the selected IP address, the first URL to the first web server, and receiving, from the first web server, the first content.

184. In my opinion, Cohen discloses or renders obvious this limitation. As discussed in explained for Limitation 1[c], the process of proxy redirector 104 sending the GET request (containing the first URL, e.g. “/a/ya/yahoomail/promo1.gif HTTP/1.0”) to the origin server (e.g. origin server 107 or 109) includes proxy cache 110-1 (the claimed “client device addressed by the selected IP address”) sending the first URL to the web server through a TCP connection that “is established between the proxy cache and the origin server to obtain a copy of the requested object.” EX1004, 7:27-35.

185. As explained for Limitations 1[d], proxy cache 110-1 receives from the origin server corresponding to the first URL the web page corresponding to the first URL from the origin and proxy redirector 104 receives the web page from proxy cache 110-1. EX1004, 8:55-58; *see also id.*, 6:39-46, 10:23-25, 12:18-20.

5. Claim 5: The method according to claim 3, wherein the receiving of the first content from the first web server comprises receiving the first content from the client device addressed by the selected IP address.

186. In my opinion, Cohen discloses or renders obvious this limitation. As explained in Limitation 1[d], proxy redirector 104 (the claimed “first server”) receives the web page corresponding to the first URL (the claimed “first content”) from proxy cache 110-1 (the claimed “client device addressed by the selected IP address”). See Fig. 1.



6. Claim 6: The method according to claim 2, further comprising communicating, by the first server, with each of the client devices that are identified over the Internet using by the stored IP addresses.

187. In my opinion, Cohen discloses or renders obvious this limitation. Proxy redirector 104 (the claimed “first server” establishes and maintains connections to determine availability, and thereby communicates, with each of the proxy caches 110-1, 110-2, 115, and/or 117, (the claimed “each of the client devices”). EX1004, 7:36-48; As discussed in Section X.C, a POSITA would understand that when proxy redirector 104 “selects one of the available proxy caches [e.g. 110-1, 110-2, 115, and/or 117] to which to forward client requests based on a metric such as least-loaded or round-robin, [or] based on IP header information such as the origin server IP address” such connection necessarily requires, or at a minimum renders obvious, proxy redirector 104 storing a list the IP addresses of the proxies. EX1004, 7:36-48; *see also id.*, 2:15-20. Further, a POSITA would also understand that when proxy redirector 104 “transparently establishes a TCP connection between the client and a proxy” such connection necessarily requires, or at a minimum renders obvious, proxy redirector 104 storing the IP address of the proxy, as this IP address is needed to be placed in the destination address field of the IP packet. *Id.*, 7:12-17.

7. Claim 7: The method according to claim 6, further comprising storing, by the first server, the IP addresses of each of the client devices in response to the communicating.

188. In my opinion, Cohen discloses or renders obvious this limitation. As discussed in Section X.C and for Claim 6, a POSITA would understand that when the proxy redirector 104 selects one of the available proxy caches (e.g. 110-1, 110-2, 115, and/or 117) it necessarily requires, or at a minimum renders obvious, proxy redirector 104 storing a list the IP addresses of proxies 110-1, 110-2, 115, and/or 117 so that it can send a IP message to them.

8. Claim 8: The method according to claim 6, further comprising receiving a ‘keep alive’ message, by the first server, from each of the client devices that are identified over the Internet using by the stored IP addresses.

189. In my opinion, Cohen discloses or renders obvious this limitation. Table 1 (annotated below), the proxy redirector establishes “keep alive” connection with the client (e.g. 101-1) and the proxies. EX1004, 11:12-15.

TABLE 1

Arriving packet:

```

---> beginning of packet header dump <---
---> IP header: version=4 hdr_len=5 TOS=0 pkt_len=346 id=60276
      frag_off=4000H TTL=64 protocol=6 cksum=1792H
      saddr=135.104.25.243 daddr=204.71.200.244
---> TCP header: sport=1273 dport=80 seq=2189084427 ack_seq=3266449517
      tcp_hdr_len=5 flags=ACK PSH
      res1=0H res2=0H window=31856 cksum=162H urgent=0
---> beginning of packet data dump <---
GET /a/ya/yahoomail/promo1.gif HTTP/1.0
Referer: http://www.yahoo.com/
Connection: Keep-Alive
User-Agent: Mozilla/4.05 [en] (X11; U; Linux 2.1.103 i686)
Host: us.yimg.com
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg image/png
Accept-Language: en
Accept-Charset: iso-8859-1, *,utf 8
Modified to:

```

```

---> beginning of packet header dump <---
---> IP header: version=4 hdr_len=5 TOS=0 pkt_len=367 id=60276
      frag_off=4000H TTL=64 protocol=6 cksum=1792H
      saddr=135.104.25.245 daddr=135.104.25.31
---> TCP header: sport=5000 dport=7000 seq=2189084427 ack_seq=3266449517
      tcp_hdr_len=5 flags=ACK PSH
      res1=0H res2=0H window=31856 cksum=162H urgent=0
---> beginning of packet data dump <---
GET http://204.71.200.244/a/ya/yahoomail/promo1.gif HTTP/1.0
Referer: http://www.yahoo.com/
Connection: Keep-Alive
User-Agent: Mozilla/4.05 [en] (X11; U; Linux 2.1.103 i686)
Host: us.yimg.com

```

190. A POSITA would understand that these HTTP keep alive messages are defined in RFC 2068 according to EX1005, 106/114. This HTTP “keep-alive” feature allows the HTTP client (e.g. client 101-1 or proxy cache) to send multiple request/response pairs over the same TCP connection. This decreases latency for subsequent HTTP requests since the proxy redirector 104 (the claimed “first server”)

doesn't close the TCP connection after each response but waits some time to allow for additional HTTP requests.

191. A POSITA would have been motivated to use this "keep-alive" functionality with each of the proxy caches (e.g. 110-1, 110-2, 115, and/or 117) to help maintain TCP connections by preventing periods of inactivity and avoid unnecessarily expending resources to reestablish connections for each HTTP request.

9. Claim 9: The method according to claim 2, wherein each of the IP addresses in the group is associated with a respective client device that is identified over the Internet using a respective IP address and is currently online.

192. In my opinion, Cohen discloses or renders obvious this limitation. As described in Claim 8, Cohen discloses keep-alive messages for the HTTP connections between the proxy redirector 104 and clients 101-1 – 101-N and between proxy redirector 104 and proxy caches 110-1, 110-2, 115, and/or 117. A POSITA would understand that the purpose of keep alive message is to know if the connection was still established. A POSITA would consider a live connection to be currently online, and likewise remove a dead connection from the list of IP addresses as to prevent an error resulting from trying to send messages over a dead connection.

10. Claim 10: The method according to claim 2, further comprising establishing, by the first server, a Transmission Control Protocol (TCP)

connection with each of the client devices that are identified over the Internet using the IP addresses in the group.

193. In my opinion, Cohen discloses or renders obvious this limitation.

Table 1 shows that the arriving packet has a protocol value of 6. A POSITA would know that protocol 6 is reserved for TCP.

TABLE 1

Arriving packet:

```
---> beginning of packet header dump <---
---> IP header: version=4 hdr_len=5 TOS=0 pkt_len=346 id=60276
      frag_off=4000H TTL=64 protocol=6 cksum=1792H
      saddr=135.104.25.243 daddr=204.71.200.244
---> TCP header: sport=1273 dport=80 seq=2189084427 ack_seq=3266449517
      tcp_hdr_len=5 flags=ACK PSH
      res1=0H res2=0H window=31856 cksum=162H urgent=0
---> beginning of packet data dump <---
GET /a/ya/yahoomail/promo1.gif HTTP/1.0
Referer: http://www.yahoo.com/
Connection: Keep-Alive
User-Agent: Mozilla/4.05 [en] (X11; U; Linux 2.1.103 i686)
Host: us.yimg.com
Accept: image/gif, image/x-bitmap, image/jpeg, image/png
Accept-Language: en
Accept-Charset: iso-8859-1, *,utf 8
Modified to:
```

```
---> beginning of packet header dump <---
---> IP header: version=4 hdr_len=5 TOS=0 pkt_len=367 id=60276
      frag_off=4000H TTL=64 protocol=6 cksum=1792H
      saddr=135.104.25.245 daddr=135.104.25.31
---> TCP header: sport=5000 dport=7000 seq=2189084427 ack_seq=3266449517
      tcp_hdr_len=5 flags=ACK PSH
      res1=0H res2=0H window=31856 cksum=162H urgent=0
---> beginning of packet data dump <---
GET http://204.71.200.244/a/ya/yahoomail/promo1.gif HTTP/1.0
Referer: http://www.yahoo.com/
Connection: Keep-Alive
User-Agent: Mozilla/4.05 [en] (X11; U; Linux 2.1.103 i686)
Host: us.yimg.com
```

194. Cohen refers throughout to the use of TCP/IP, including with respect to the proxy redirector 104 (“first server”) and the client devices. For example, “once the IP address of the origin server corresponding to the logical URL name is determined through the DNS look-up, proxy redirector 104, rather than establishing

a TCP connection to the origin server at the determined IP address, transparently establishes a TCP connection between the client and a proxy.” EX1004, 7:12-17.

195. Cohen also describes that “[i]n establishing a TCP connection that is directed to an origin server, client 101-1 first transmits a SYN packet, which is intercepted by proxy redirector 104.” EX1004, 8:59-61; *see also* EX1004, 15:5-8 (“Similarly, in all packets received by the proxy redirector from the client directed to the origin server within a persistent TCP connection, the seq parameter must reflect cumulative changes.”). Further, the connection control block (CCB) created by the proxy redirector “is used to store the client IP address and TCP port number.” EX1004, 8:66-67. Thus, a POSITA would understand that Cohen’s disclosure of proxy redirector 104 communicating with the proxy caches discloses or renders obvious proxy redirector establishing a TCP connection with each of the proxy caches.

11. Claim 11: The method according to claim 1, further comprising by the first server: sending, a ‘keep alive’ message to each of the client devices that are identified over the Internet using by the stored IP addresses; and waiting for a response to the ‘keep alive’ message from each of the client devices

196. In my opinion, Cohen discloses or renders obvious this limitation. This limitation is just a recitation of the well-known algorithm for keep alives. As discussed in Claim 8, proxy redirector (the claimed “first server”) sends keep-alive

messages to the proxy caches (the claimed “client devices”) and it must wait for response from each of them to know they are still alive.

12. Claim 12: The method according to claim 11, further comprising responsive to not receiving, by the first server, a response to the ‘keep alive’ message from a client device, removing the IP address of the non-responsive third client device from group of IP addresses

197. In my opinion, Cohen discloses or renders obvious this limitation. As discussed in Claims 8 and 9, it would have been obvious remove the IP address of a non-responsive client device from the list of IP addresses of devices under active session.

13. Claim 13: The method according to claim 11, wherein the sending of the ‘keep alive’ message comprises periodically sending by the first server the ‘keep alive’ message to at least part of the client devices.

198. In my opinion, Cohen discloses or renders obvious this limitation. As discussed in Claim 8, the proxy redirector 104 (the claimed “first server”) periodically sends keep-alive messages to the proxy caches (the claimed “client devices”).

14. Claim 14: The method according to claim 1, for use with a criterion stored in the first server, wherein the selecting is according to, or based on, the criterion.

199. In my opinion, Cohen discloses or renders obvious this limitation. As explained in Limitations 1[b] and 1[f], a POSITA would have understood that, proxy director 104 uses a stored criterion when it selects one of the available proxy

caches to which to forward client requests based on a metric, such as least-loaded or round-robin.

(“Proxy redirector 104 **selects** one of the available proxy caches to which to forward client requests **based on a metric such as least-loaded or round-robin**, based on IP header information such as the origin server IP address.”)

EX1004, 7:36-48;

15. Claim 17: The method according to claim 14, wherein the criterion is based on, or comprises, a response time when communicating.

200. In my opinion, Cohen discloses or renders obvious this limitation. A POSITA would have understood that, “a metric such as least-loaded” is based on a response time when communicating, as response time is a common method of measuring a server’s load. EX1004, 7:36-48.

16. Claim 20: The method according to claim 1, further comprising sending the received first content to the first client device.

201. In my opinion, Cohen discloses or renders obvious this limitation. See Limitation 1[d].

17. Claim 21: The method according to claim 20, further comprising sending the received second content to the first client device

202. In my opinion, Cohen discloses or renders obvious this limitation. See Claim 1[h].

18. Claim 22: The method according to claim 1, wherein the first client device is addressed over the Internet using a first Internet Protocol (IP) address,

and the method further comprising storing, in the first server, the first IP address.

203. In my opinion, Cohen discloses or renders obvious this limitation. The first client device is addressed over the Internet using a first Internet Protocol address, Table 2 shows the addressing of the client by IP address, 135.104.25.243. See Claim 6.

TABLE 2

Arriving packet:

```
---> beginning of packet header dump <---  
---> IP header: version=4 hdr_len=5 TOS=0 pkt_len=40 id=14559  
      frag_off=4000H TTL=255 protocol=6 cksum=10eH  
      saddr=135.104.25.31 daddr=135.104.25.245  
---> TCP header: sport=7000 dport=5000 seq=3266449517 ack_seq=2189084754  
      tcp_hdr_len=5 flags=ACK  
      res1=0H res2=0H window=8433 cksum=32H urgent=0
```

Modified to:

```
---> beginning of packet header dump <---  
---> IP header: version=4 hdr_len=5 TOS=0 pkt_len=40 id=14559  
      frag_off=4000H TTL=255 protocol=6 cksum=10eH  
      saddr=204.71.200.244 daddr=135.104.25.243  
---> TCP header: sport=80 dport=1273 seq=3266449517 ack_seq=2189084733  
      tcp_hdr_len=5 flags=ACK  
      res1=0H res2=0H window=8433 cksum=32H urgent=0
```

19. Claim 23: The method according to claim 1, wherein the first server is a Transmission Control Protocol/Internet Protocol (TCP/IP) server that communicates over the Internet with client devices based on, according to, or using, TCP/IP protocol or connection.

204. In my opinion, Cohen discloses or renders obvious this limitation. As discussed for Limitations 1[p] proxy redirector 104 (the claimed “first server”) is a

server” and, as discussed for Claim 10, Cohen discloses or renders obvious proxy redirector 104 communicating with the proxy caches (the claimed “client devices”) over the Internet using TCP/IP.

20. Claim 24: The method according to claim 1, wherein the first server communicates over the Internet based on, or according to, one out of UDP, DNS, TCP, FTP, POP#, SMTP, or SQL standards.

205. In my opinion, Cohen discloses or renders obvious this limitation, as it discloses the proxy redirector communicating over the Internet using TCP. As discussed in Claim 23, a POSITA would understand that all requests from the clients disclosed in Cohen to servers connected to the Internet “traverse proxy redirector 104 onto the Internet.” EX1004, 6:31-34. The same is true for responses. EX1004, 6:39-46. And in both cases, “standardized packets that establish a TCP connection” are utilized. EX1004, 6:31-46.

21. Claim 26: The method according to claim 1, for use with a second client device, the method further comprising, by the first server: receiving a message from the second client device; and responsive to the receiving of the message from the second client device, adding the IP address of the second device to the group of IP addresses.

206. In my opinion, Cohen discloses or renders obvious this limitation, as it discloses the proxy redirector communicating with all of the clients, 101-1 – 101-N.

(“**All requests from any of the clients** connected to LAN 102 for objects stored in servers connected to the Internet 105 **traverse proxy redirector 104** onto the Internet.”) EX1004, 2:31-34.

207. A POSITA would understand that a second client computer (e.g. 101-2) could establish a connection through proxy redirector 104, with proxy redirector 104 performing the same steps as described in Limitations 1[a]-1[g] above.

22. Claim 27: *The method according to claim 1, wherein the sending of the first URL to the first web server comprises using the selected IP address as a source address.*

208. In my opinion, Cohen discloses or renders obvious this limitation. As discussed for Limitation 1[c], under the **PO Construction** of “source address,” when by proxy cache (e.g. 110-1) further forwards towards the origin server, the IP address associated with proxy cache 110-1 is used as the “source address.”

23. Claim 28: *The method according to claim 1, further comprising sending, by the first server, the selected IP address in response to the selecting.*

209. In my opinion, Cohen discloses or renders obvious this limitation. As explained in Claim 1[c], proxy redirector 104 sends the URL to proxy cache 110-1 in response to the selecting. As explained for Claim 6, when proxy redirector 104 sends IP packets to proxy cache 110-1, it uses the IP address of proxy cache 110-1 (the claimed “selected IP address”) as the “destination address.” The “destination address” is part of the IP header and is thus sent with the IP packet. *See also* EX1015, 17/51; EX1016, 57/91.

24. Claim 29: *The method according to claim 1, wherein the first client device is identified by a first Internet Protocol (IP) address, Media Access Control (MAC) address, or a hostname*

210. In my opinion, Cohen discloses or renders obvious this limitation. Cohen discloses how a “first client device” (client 101-1) is identified by a first IP address—specifically its own IP address—in sessions with proxy redirector 104, as shown in Table 2.

TABLE 2

Arriving packet:

```
---> beginning of packet header dump <---  
---> IP header: version=4 hdr_len=5 TOS=0 pkt_len=40 id=14559  
      frag_off=4000H TTL=255 protocol=6 cksum=10eH  
      saddr=135.104.25.31 daddr=135.104.25.245  
---> TCP header: sport=7000 dport=5000 seq=3266449517 ack_seq=2189084754  
      tcp_hdr_len=5 flags=ACK  
      res1=0H res2=0H window=8433 cksum=32H urgent=0
```

Modified to:

```
---> beginning of packet header dump <---  
---> IP header: version=4 hdr_len=5 TOS=0 pkt_len=40 id=14559  
      frag_off=4000H TTL=255 protocol=6 cksum=10eH  
      saddr=204.71.200.244 daddr=135.104.25.243  
---> TCP header: sport=80 dport=1273 seq=3266449517 ack_seq=2189084733  
      tcp_hdr_len=5 flags=ACK  
      res1=0H res2=0H window=8433 cksum=32H urgent=0
```

25. Claim 30: *The method according to claim 1, further comprising storing, operating, or using, by the first server, a server operating system.*

211. In my opinion, Cohen discloses or renders obvious this limitation. Cohen discloses that the proxy redirector can be a programmable network element, which runs on a Linux machine.

(“In the preferred embodiment described herein, **proxy redirector 104** includes a **programmable network element** of the type described in co-pending U.S. patent application Ser. No. 09/190,355, filed Nov. 12, 1998, which application is incorporated herein by reference. As described in that application, **that programmable network element in the preferred embodiment runs on a Linux machine.**”) EX1004, 7:49 – 55.

212. A POSITA would know that Linux is a type of operating system, therefore the first server must be operating or using a server operating system.

26. Claim 31: *The method according to claim 1, for use with a software application that includes computer instructions that, when executed by a computer processor, cause the processor to perform the steps of the claim 1*

213. In my opinion, Cohen discloses or renders obvious this limitation. Cohen discloses that the functions described can be software (“computer readable medium”) executed by computer or processor.

(“Thus, for example, it will be appreciated by those skilled in the art that the block diagrams and flowcharts described hereinabove represent conceptual views of illustrative circuitry and processes embodying the principles of the invention. Similarly, it will be appreciated that **any flowcharts, flow diagrams, state transition diagrams, pseudocode, and the like represent various processes which may be substantially represented in computer**

readable medium and so executed by a computer or processor, whether or not such a computer or processor is explicitly shown.”) EX1004, 17:32-41.

27. Claim 32: *The method according to claim 1, wherein the first web server comprises a web server that is a Hypertext Transfer Protocol (HTTP) server responding to HTTP requests and addressed in the Internet using a web server Internet Protocol (IP) address.*

214. In my opinion, Cohen discloses or renders obvious this limitation.

Cohen discloses that the origin server is an HTTP web server.

(“In order to transparently redirect an **HTTP connection request that is directed to an origin server (107)** to a proxy cache (110-1), a proxy redirector (104) translates the destination address of packets directed to the origin Server to the address of the proxy.”) EX1004, Abstract.

215. A POSITA would understand Cohen’s disclosure of web requests and responses to disclose HTTP requests and responses. For example, Cohen explains that “HTTP connection requests are generally directed to port 80 of an origin server.” EX1004, 3:3-4. Table 1 of Cohen and the surrounding text illustrates an example “HTTP” request directed to a web server at www.yahoo.com with a particular IP address. EX1004, Table 1, 10:33-11:23.

XII. Conclusion

216. I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

3/13/2022

Date

James Olivier Ph.D.

James Olivier, Ph.D.

PROFESSIONAL SUMMARY

The foundation for my career began over thirty years ago with a Doctorate in Electrical Engineering.

I am currently an Adjunct Professor Telecommunications and Network Engineering Program Southern Methodist University's Graduate School of Electrical Engineering, where I teach MPLS enabled applications to graduate students. I am also the owner of Olivier Consulting, where I provide consulting services for advanced network / system design along with IP consulting. In addition, I am also a member of the technical staff of McAlexander Sound, where I specialize in Telecommunications Architecture / Computer Software. Recently I have been appointed Program Lead and Adjunct Executive in Residence at SMU's Hunt Institute for Engineering and Humanity for Transformational Technologies.

I have three degrees from The Ohio State University: a Bachelor of Science degree in Electrical Engineering; a Master of Science degree in in Electrical Engineering and a Doctor of Philosophy degree in Electrical Engineering. I have published papers in the areas of coding theory and multiprocessor computer systems.

Over the last 18 years I have devoted my attention to industry consulting in the areas of intellectual property and networking technologies.

EDUCATION PROFILE

Ph.D. Electrical Engineering, The Ohio State University, Columbus, Ohio, 1988 Dissertation: "*Concurrent Error Detection in Arithmetic Processors using GAN Codes*", Received separate minors in fields of Computer Science, Microelectronics and Semiconductor Fabrication, and Discrete Mathematics.

Recipient of the prestigious Kodak Fellowship, awarded nationally to 12 doctoral students in the fields of science and engineering.

MS. Electrical Engineering, The Ohio State University, Columbus, Ohio, 1985 Thesis: "*A Navigation System for a Vehicle with a Laser Rangefinder*"; Major areas of study were robotics and artificial intelligence.

BS. Electrical Engineering, The Ohio State University, Columbus, Ohio, 1983 Cum Laude.

EXPERIENCE PROFILE

2019 – present **Program Lead and Adjunct Executive in Residence SMU's Hunt Institute for Engineering and Humanity Southern Methodist University**

- Program Lead of Hunt Institute's Transformational Technology Hub responsible for strategy formulation and project implementation.

2017 - present **Adjunct Professor Telecommunications and Network Engineering Program Southern Methodist University's Lyle School of Electrical Engineering**

- Teaching Advanced Switching and Routing with MPLS at SMU's nationally rated Telecommunications and Network Engineering program. Research interests include SDNs, Video Transport, SD-WANs, Blockchain, IoT, and In-Networking Processing.

2003 - present **Olivier Consulting – Dallas Texas
IP Consultant M^cAlexander Sound**

- Technology Research and Intellectual Property Management, including, IP Protection, IP Validity, IP Portfolio Valuation, IP Strategy and IP Technical Consultation. Clients include Arista Networks, HTC Corporation, T-Mobile, Samsung, Vizio, Google Corporation, Level 3 Communications, AT&T, Amazon, Ericsson, and S.T Microelectronics.

Recognized Expert before United States Federal District Courts in the Areas of

- Congestion Control in Packet Switching
QPSX v Nortel 2:05-CV-268, 2007
- Cellular High Speed Packet Access Networks
Wi-LAN Inc., v. Alcatel-Lucent et. al CV-6:10, 2013
- Signaling Protocols in Cellular Networks
Core Wireless Licensing S.A.R.L v. Apple 6:12-CV-100, 2015

Recognized Expert before the International Trade Commission in the Areas of

- Security and Firewalls in Routers and Switches;
Investigation 337-TA-628, 2007
- Cellphone Hardware and Software for Imaging;
Investigation 337-TA-726, 2010
- Operating Systems for Mobile Devices;
Investigation 337-TA-744, 2011
- Mobile Devices Hardware and Software Architectures;
Investigation 337-TA-850, 2012
- Ethernet Switch Packet Processor Hardware and Software;
Investigation 337-TA-945, 2015

Lead Technology Research and Intellectual Property investigations in the following areas

- Technology related to mobile camera system's software systems architecture. *HTC Corporation*
- Technology related to gateway protocols between Cellular /PSTN Networks and the Internet. Investigated the design of a Packet Gateway and associated soft switch. *Level 3 Communications*
- Technology related to content delivery server systems based on demographic information received from client systems. *AT&T*
- Technology investigation related to Metro Ethernet, MPLS, 802.17, and 802.3 access products. *Transpacific IP*
- Technology investigation related to the research, specification, design, and architecture of the Telstrat's Next Generation Switch, which provided video, including analog, digital, HDTV, along with IP based voice, and also provided internet service. *Telstrat*
- Technology investigation into the specification, design, and architecture of the Crane Wireless Sensor Network. Investigated scalability, address assignment, access, and security for a large IoT Wireless Sensor Network. *Crane Aerospace*

2002 - 2003 Navini Networks - Richardson, Texas Senior Manager

- Performed research and development in Navini's Wireless CDMA broadband System. Responsible for definition and implementation of layer 2 and layer 3 network protocols for Navini's Broadband Wireless Products. Developed servers for network security, network services, service provisioning and subscriber management for a CDMA network. Responsible for the design and development of a sign-on web site which managed and authorized users for different services in a broadband CDMA network. This system consisted of multiple Apache Web Servers providing the web pages to the users and a centralized key storage facility to manage the various keys needed to authorize the different services.

1999 – 2002 Marconi Communications - Irving, Texas Manager of Systems Engineering

- Responsible for design and development of new products and product evolution for Marconi's North American Access Division. I developed systems for the access video market, such as Digital Subscriber Line (DSL) networks, Hybrid fiber-coaxial (HFC) networks and DOCSIS systems. These systems were triple play systems which provide voice, video and data. While at Marconi, I was also responsible for the web servers design for the Network Management System for the North American Access product division.

1996– 1999 Samsung Telecommunications America - Richardson, Texas Principal Engineer

- Responsible for Service Control subsystem of Samsung's next generation wireless broadband UMTS switching system. Designed and developed a Java based platform for defining services for Samsung's next generation high-speed wireless switch. Areas of responsibility include traditional telephony services, wireless services, broadband services, and Internet services, such as an email portal. While at Samsung, I was also their corporate representative to the International Telecommunication Union, ("ITU"), which is the agency of the United Nations responsible for information and communication technologies. I was also Samsung's corporate representative to the 3GPP standards

body. It was there that I participated in the development of standards for advanced wireless networks, including multimedia transport.

1995 – 1996 **DSC Switch Products Division – Plano, Texas**

Senior Manager: Intelligent Network Evolution and Business Planning

- Responsible for architecture and development of DSC's Intelligent Network product line. These products demonstrated at SuperComm 1996; a U.S. telecommunications trade show showed the integration of streaming media servers together with the interactivity of the Internet. I also actively interacted with key customers on their system designs and participated in relevant standards work.

Senior Manager: ATM Systems Engineering Group

- Lead the systems engineering group in defining a new high-speed ATM switches for enterprise and telecommunication networks. These efforts include, multiprocessor architectures, communications subsystems, and software architectures. In addition, I was responsible for responding to RFIs and RFPs for a number of clients server based multimedia systems and served as DSC corporate representative to the ATM Forum.

1990 – 1995 **AT&T Bell Laboratories - Columbus, Ohio**
Member of Technical Staff

- Designed and implemented a variety of multiprocessor systems for use in the computer/multimedia systems. These systems included Asynchronous Transfer Mode 'ATM' based Internet and video distribution system. I also participated in the design and development of client server based systems for database access. At this time, I also began my work with standard settings bodies. While at AT&T Bell Laboratories in 1990s, I was charged with monitoring standard setting bodies such as the ATM Forum and DAVIC, the Digital Audio-Visual Council.

1989 – 1990 **General Motors Research Laboratories Warren
Michigan**

**Senior Research Engineer: Computer Science
Department**

- Conducted research into basic computer science problems associated with the future development of vehicular systems. These areas include the design of fault tolerant control systems, new cost affective microprocessor architectures and software for reliability and performance modeling. Lead the development of an automotive testbed for the evaluation of prototype systems.

1988 – 1989 **Harris Communications – Melbourne, Florida
Principal Engineer**

- Conducted research and development into innovative computer systems for use in space systems. Studied coherency protocols for microprocessor memory systems. Developed fault tolerant multi-processor computer systems for use in Strategic Defense Initiative.

PUBLICATIONS

Olivier, J., Ozguner, F. "*A navigation algorithm for an intelligent vehicle with a laser rangefinder*", Proceedings of the 1986 IEEE International Conference on Robotics and Automation, Vol. 3, April 1986.

Olivier, J. L. and Ozguner, F. "*Design of Concurrent Error Detecting Systolic Arrays Using GAN Codes*" IEEE Transactions on Computer Aided Design, vol. 9, no. 10 October 1989.

Olivier, J.L. "*Low Cost Residue Prediction for Improved Addition Efficiency*", G. M. Research Publication, December 1989.

Olivier, J.L. and Tkacik, T.E., "*RELY, a Markov Modeling Package for System Reliability Prediction*" G.M. Research Publication, January 1990.

ISSUED PATENTS AND PATENT APPLICATIONS

- US 8334775 RFID-based asset security and tracking system, apparatus and method Network based asset management system.
- US 20090174772 Security and surveillance system
Network based surveillance and security system.
- US 20130201337 Rfid-based asset security and tracking system, apparatus and method
Network based asset management system.

ADDITIONAL ACTIVITIES

Member of the Advisory Board for the Innovation Hub for the Dallas County Community College District.

Fellow at SMU's Hunt Institute for Engineering and Humanity.

Chairman of IEEE Dallas Blockchain Group

Cases Worked Past 10 Years

Year Engaged

2022

Expert Engagement: IPR
Type of Matter: Inter partes review
Case Name: PTAB IPR on
U.S. Patent No. 7,623,003 and 8,766,797
Engaged on behalf of: Qualcomm
Technology at Issue: Sensor networks
Services Provided: Wrote Declaration
Law Firm: Norton Rose
Year Engaged: 2022

Expert Engagement: Litigation
Type of Matter: Inter partes review
Case Name: PTAB IPR on
U.S. Patent No. 10,325,159
Engaged on behalf of: Vivint
Technology at Issue: Electronic Monitoring
Services Provided: Wrote Declaration
Law Firm: Foley and Lardner
Year Engaged: 2022

2021

Expert Engagement: Litigation
Type of Matter: Inter partes review
Case Name: PTAB IPR on
U.S. Patent No. 9,549,426
Engaged on behalf of: Ericsson
Technology at Issue: Signaling Messages in cellular networks
Services Provided: Consulting
Law Firm: Baker Botts

Year Engaged: 2021

Expert Engagement: Litigation
Type of Matter: Inter partes review
Case Name: PTAB IPR on
U.S. Patent No. 7,979,070
Engaged on behalf of: Thales AIS DIS
Technology at Issue: Signaling Messages in 3GPP networks
Services Provided: Wrote Declaration
Law Firm: AddyHart LLP
Year Engaged: 2021

Expert Engagement: Litigation
Type of Matter: Inter partes review
Case Name: PTAB IPR on
U.S. Patent No. 10,346,114
Engaged on behalf of: Roku, Inc.
Technology at Issue: Content delivery over wireless networks
Services Provided: Wrote Declaration
Law Firm: Perkins Coie
Year Engaged: 2021

Expert Engagement: Litigation
Type of Matter: Inter partes review
Case Name: PTAB IPR on
U.S. Patent No. 7,580,388
Engaged on behalf of: Thales AIS DIS
Technology at Issue: Signaling Messages in 3GPP networks
Services Provided: Wrote Declaration
Law Firm: AddyHart LLP
Year Engaged: 2021

Expert Engagement: PTAB

Type of Matter: Inter partes review
Case Name: PTAB IPR on
U.S. Patent No. 9,54,426
Engaged on behalf of: Ericsson Inc.
Technology at Issue: Signaling Messages in GSM networks
Services Provided: Wrote Declaration
Law Firm: Baker Botts
Year Engaged: 2021

Expert Engagement: PTAB
Type of Matter: Inter partes review
Case Name: PTAB IPR on
U.S. Patent No. 10,601,948
Engaged on behalf of: Metacluster
Technology at Issue: Computer networks
Services Provided: Wrote Declaration
Law Firm: Norton Rose
Year Engaged: 2021

2020

Expert Engagement: Litigation
Type of Matter: Patent
Case Name: Intellectual Ventures I LLC and Intellectual Ventures II LLC
v. VMware, Inc., Western District of Texas Case No. 6:19-
cv-449
Engaged on behalf of: VMware
Technology at Issue: Layer 3 Networking
Services Provided: Wrote Declaration
Law Firm: Winston & Strawn
Year Engaged: 2020

Expert Engagement: Litigation
Type of Matter: Patent

Case Name: Exafer Ltd. v. Microsoft Corporation, Case No: 20-CV-00131 ADA
Engaged on behalf of: Microsoft
Technology at Issue: Layer 2 forwarding
Services Provided: Wrote Declaration
Law Firm: Winston & Strawn
Year Engaged: 2020

Expert Engagement: Litigation
Type of Matter: Copyright
Case Name: Apple Inc. v Corellium, LLC
CASE NO. 9:19-cv-81160-rs Southern District of Florida
Engaged on behalf of: Corellium LLC
Technology at Issue: Software and image copyrights
Services Provided: Wrote Declaration, attended deposition
Law Firm: Hecht Partners LLP
Year Engaged: 2020

Expert Engagement: Litigation
Type of Matter: Inter partes review
Case Name: PTAB IPR on
U.S. Patent No. 7,894,443
Engaged on behalf of: Thales AIS DIS
Technology at Issue: Radio Link Control
Services Provided: Wrote Declaration
Law Firm: AddyHart LLP
Year Engaged: 2020

Expert Engagement: Litigation
Type of Matter: Inter partes review
Case Name: Sisvel International S.A. and 3G Licensing S.A. v. Cradlepoint, Inc., Case No. 1:19- CV-1142-MN (District of Delaware)
Engaged on behalf of: Cradlepoint and Sierra Wireless
Technology at Issue: Radio Link Control
Services Provided: Wrote Declaration

Law Firm: Perkins Coie
 Year Engaged: 2020

Expert Engagement: PTAB Case No. IPR2021-00260
 Type of Matter: Inter partes review
 Case Name: PTAB IPR on U.S. Patent No. 9, 723,813 to Davis
 Engaged on behalf of: Tomofun
 Technology at Issue: Animal Interaction System
 Services Provided: Wrote Declaration
 Law Firm: Greenberg Traurig, LLP
 Year Engaged: 2020

2019

Expert Engagement: Litigation
 Type of Matter: Patent Investigation
 Case Name: SIMO Holdings v Hong Kong uCloudlink Networks Technology Limited and uCloudlink (America) LTD.
 CASE NO. 1:18-cv-05427 Southern District NY
 Engaged on behalf of: uCloudlink Ltd
 Technology at Issue: Wireless data links
 Services Provided: Wrote Declarations
 Law Firm: Fish & Richardson

Year Engaged: 2019

Expert Engagement: Litigation
 Type of Matter: Patent Investigation
 Case Name: Harris Corporation v. Huawei Device USA, Inc., et al.
 Case No. 2:18-cv-439 ED-TX
 Engaged on behalf of: Huawei Device USA
 Technology at Issue: Network Security
 Services Provided: Wrote Declaration, Gave Deposition testimony
 Law Firm: Ropes & Gray LLP
 Year Engaged: 2019

2018

Expert Engagement: Inter Partes Review
Type of Matter: Patent Review
Case Number: IPR2017-00829, -00830, -01131, -01133
Engaged on behalf of: Vidstream LLC
Technology at Issue: Networked Video
Services Provided: Wrote Declaration, attended deposition
Law Firm: Norton Rose
Year Engaged: 2018

Expert Engagement: Litigation
Type of Matter: Patent Investigation
Case Name: Arista Networks, Inc. v. Cisco Systems, Inc. No. 5:16-CV-00923-BLF (N.D. Cal.)
Engaged on behalf of: Arista Networks
Technology at Issue: Network protocols
Services Provided: Signed Declaration
Law Firm: Tensegrity Law Group
Year Engaged: 2018

Expert Engagement: Litigation
Type of Matter: Patent Investigation
Case Name: Intellectual Ventures I LLC v. HCC Insurance Holdings Inc. CA No. 6:15-cv-00660 ED-TX
Engaged on behalf of: HCC Insurance Holdings
Technology at Issue: Back end web site technology
Services Provided: Wrote expert report, attended deposition
Law Firm: Norton Rose Fulbright
Disposition: Settled
Year Engaged: 2018

2017

Expert Engagement: Inter Partes Review
 Type of Matter: Patent Review
 Case Number: IPR2018-00287
 Engaged on behalf of: Comtech Mobile Datacom Corporation
 Technology at Issue: Vehicle Mapping Technology
 Services Provided: Wrote Declaration
 Law Firm: Perkins Coie LLP
 Year Engaged: 2017

Expert Engagement: ITC Matter
 Type of Matter: Patent Investigation
 Case Name: ITC Inv.No.337-TA-1057 Certain Robotic Vacuum Cleaning
 Devices and Components Thereof
 Such as Spare Parts,
 Engaged on behalf of: Shenzhen Silver Star Intelligent Technology
 Technology at Issue: Autonomous Vehicle Technology
 Services Provided: Wrote expert report, gave deposition and hearing testimony
 Law Firm: Pillsbury Winthrop Shaw Pittman
 Year Engaged: 2017

2016

Expert Engagement: Litigation and Inter Partes Review
 Type of Matter: Patent Investigation
 Case Name: International Business Machines Corp. v. The Priceline
 Group Inc., et al C.A. No. 15-137-LPS, and IPR2016-00608
 and IPR2016-00609.
 Engaged on behalf of: The Priceline Group Inc.
 Technology at Issue: Web site Technology
 Services Provided: Wrote Expert Reports on Invalidity and Non-infringement.
 Attended Deposition.
 Law Firm: Norton Rose Fulbright
 Year Engaged: 2016

Expert Engagement: Litigation
 Type of Matter: Patent Investigation
 Case Name: Evolv, LLC v. Joyetech USA, Inc.
 Case No. 8:16-cv-00459-CJC-JCG CD-CA
 Engaged on behalf of: Joytech USA
 Technology at Issue: Computer controlled voltage source
 Services Provided: Wrote Declaration
 Law Firm: Pillsbury Winthrop Shaw Pittman LLP
 Disposition: Settled
 Year Engaged: 2016

Expert Engagement: Inter Partes Review
 Type of Matter: Patent Review
 Case Number: IPR2016-01431
 Engaged on behalf of: HCC Insurance Holdings
 Technology at Issue: Web site design; Network Agent Technology
 Services Provided: Wrote Declarations for IPR
 Law Firm: Norton Rose Fulbright
 Disposition: Settled
 Year Engaged: 2016

2015

Expert Engagement: Litigation
 Type of Matter: Patent Investigation
 Case Name: Advanced Media Networks, LLC v. AT&T Mobility LLC.
 C.A. NO. 3:15-cv-03496-N ND-TX
 Engaged on behalf of: Advanced Media Networks
 Technology at Issue: Mobile Hotspots
 Services Provided: Wrote Declarations, attended deposition
 Law Firm: Buether Joe and Carpenter
 Year Engaged: 2015

Expert Engagement:

Type of Matter: Inter Partes Review
Case Number: IPR2016-01255, - 01253
Engaged on behalf of: Advanced Media Networks
Technology at Issue: Mobile Hotspots
Services Provided: Wrote Declarations
Law Firm: Buether Joe and Carpenter
Year Engaged: 2015

Expert Engagement:

Type of Matter: Inter Partes Review
Type of Matter: Patent Review
Case Number: IPR2016-00032,-0033
Engaged on behalf of: USAA Federal Savings Bank
Technology at Issue: Secure Transactions Technology
Services Provided: Wrote Declaration for IPR
Law Firm: Norton Rose Fulbright
Year Engaged: 2015

Expert Engagement:

Type of Matter: ITC Investigation
Type of Matter: Patent Investigation
Case Name: In the Matter of Certain Network Devices (II)
USITC Inv. No. 337-TA-945
Engaged on behalf of: Arista Networks
Technology at Issue: Network protocols
Services Provided: Wrote Expert Report, Gave Deposition Testimony
and Testified at Trial
Law Firm: Fish and Richardson
Year Engaged: 2015

Expert Engagement:

Type of Matter: Inter Partes Review
Type of Matter: Patent Investigation
Case Name: IPR 2014-00493 and 2014-00749

Engaged on behalf of:	Securus Technologies
Technology at Issue:	Technology related to prison telephony equipment
Services Provided:	Submitted declarations with the USPTO; Gave Deposition Testimony
Law Firm:	Fenwick & West
Year Engaged:	2015

2014

Expert Engagement:	Litigation
Type of Matter:	Patent Investigation
Case Name:	Abstrax Inc. v Hewlett_Packard Company Case No. 2:14-CV-158 Eastern District Texas
Engaged on behalf of:	Abstrax Inc.
Technology at Issue:	Computer Assisted Manufacturing
Services Provided:	Patent Analysis; Wrote Expert Report
Law Firm:	Dovel and Luner
Disposition:	Settled
Year Engaged:	2014

Expert Engagement:	Litigation
Type of Matter:	Patent Investigation
Case Name:	Solocron Media, LLC v. Verizon Communications Inc. et. al. 2:13-cv-01059 ED-Texas
Engaged on behalf of:	T-Mobile
Technology at Issue:	MMS Technology
Services Provided:	Wrote Expert Report
Law Firm:	Gibson Dunn
Disposition:	Settled
Year Engaged:	2014

Expert Engagement:	ITC Investigation
Type of Matter:	Patent Investigation

Case Name: In the Matter of Certain Wireless Devices, Including Mobile Phone and Tablets II, Inv. USITC Inv. No. 337-TA-905
 Engaged on behalf of: Samsung
 Technology at Issue: Mobile Mapping Applications
 Services Provided: Patent Analysis
 Law Firm: Fish and Richardson
 Year Engaged: 2014

Expert Engagement: Litigation
 Type of Matter: Patent Investigation
 Case Name: WAG Acquisition v. Gattyan Group Sarl; No. 2:2014cv02832 District of New Jersey
 Engaged on behalf of: Gattyan Group
 Technology at Issue: Streaming Video
 Services Provided: Patent Analysis
 Law Firm: Baker & McKenzie
 Disposition: Ongoing
 Year Engaged: 2014

Expert Engagement: ITC Investigation
 Type of Matter: Patent Investigation
 Case Name: In the Matter of Certain Point-to-Point Network Communication Devices and Products' Containing the Same
 USITC Inv. No. 337-TA-892
 Engaged on behalf of: Amtran and Vizio Corporations
 Technology at Issue: Streaming Video
 Services Provided: Wrote Expert Report on Non-Infringement; Gave Deposition Testimony
 Law Firm: Perkins Coie and Baker & McKenzie
 Year Engaged: 2014

Expert Engagement: Litigation
 Type of Matter: Patent Investigation
 Case Name: Juniper Networks, Inc., v. Fenner Investments, Ltd.

Case No. 3:11-CV-00150 Northern District of Texas
 Engaged on behalf of: Fenner Investments
 Technology at Issue: Network Security
 Services Provided: Analyzed Patents and Software
 Law Firm: Norton Rose Fulbright
 Year Engaged: 2014

Expert Engagement: Inter Partes Review
 Type of Matter: Patent Investigation
 Case Name: IPR2014-01460
 Engaged on behalf of: HTC Corporation
 Technology at Issue: Technology related to camera system architecture.
 Services Provided: Submitted declarations with the USPTO
 Law Firm: Perkins Coie
 Year Engaged: 2014

2013

Expert Engagement:
 Type of Matter: Patent Investigation
 Case Name: *In the Matter of Certain Wireless Devices with 3G and/or 4G Capabilities and Components Thereof*
USITC Inv. No. 337-TA-868
 Engaged on behalf of: Samsung
 Technology at Issue: Network protocols for cellphone power control
 Services Provided: Wrote Expert Reports on Invalidity and Non-infringement;
 Gave Deposition Testimony
 Law Firm: Ropes and Gray
 Disposition: Finding of no violation
 Year Engaged: 2013

Expert Engagement:
 Type of Matter: Patent Investigation
 Case Name: *Good Technology v. Little Red Wagon Technologies, Inc.,*
LRW Digital, Inc. and LRW Digital Inc. d/b/a LRW

Technologies, Inc. and LRW Digital, Inc., and Fixmo U.S., Inc*
Case No. 3:11-cv-02373-M Texas Northern District

Engaged on behalf of: Fixmo
 Technology at Issue: Smartphone emails and firewalls
 Services Provided: Wrote Expert Report Invalidity
 Law Firm: Gibson Dunn
 Disposition: Settled
 Year Engaged: 2013

Expert Engagement:
 Type of Matter: Patent Investigation
 Case Name: *Cradle IP LLC v Texas Instruments Incorporated*
Case No. 11-1254-SLR Delaware

Engaged on behalf of: Cradle IP LLC
 Technology at Issue: Microprocessor hardware architecture
 Services Provided: Wrote Expert Report Validity; Gave Deposition Testimony
 Law Firm: Dickstein Shapiro
 Disposition: Summary judgment of non-infringement
 Year Engaged: 2013

Expert Engagement:
 Type of Matter: Patent Investigation
 Case Name: *Smart Audio Technologies v. HTC Corporation*
Case No. 12-0221-GMS Delaware

Engaged on behalf of: HTC Corporation
 Technology at Issue: Cellphone music players
 Services Provided: Patent Analysis
 Law Firm: Perkins Coie
 Year Engaged: 2013

Level 3 Communications
 Patent evaluation services
 Technology related to Internet Technology
 Retained by Akin Gump Strauss Hauer & Feld

2012

Expert Engagement:

Type of Matter: Patent Investigation
Case Name: *Regarding Certain Electronic Imaging Devices USITC Inv. No.337-TA-850*
Engaged on behalf of: HTC Corporation
Technology at Issue: Cell phone software architecture and MMS messaging
Services Provided: Wrote Expert Reports on Invalidity and Non-infringement; Gave Deposition Testimony; Testified at Hearing
Law Firm: Perkins Coie
Disposition: Final determination of non-infringement
Year Engaged: 2012

Expert Engagement:

Type of Matter: Patent Investigation
Case Name: *Core Wireless Licensing S.A.R.L v. Apple, Inc. Case No. 6:12-CV-100-LED Eastern District of Texas*
Engaged on behalf of: Core Wireless
Technology at Issue: Network protocols for cellphone
Services Provided: Wrote Expert Reports Validity and Infringement; Gave Deposition Testimony; Testified at Trial
Law Firm: Bunsow, De Mory LLP
Disposition: Concluded
Year Engaged: 2012

AT&T

Patent evaluation services
Technology related to Content Delivery
Retained by Akin Gump Strauss Hauer & Feld

Expert Engagement:

Type of Matter: Patent Investigation
Case Name: *Wi-LAN Inc., v. Alcatel-Lucent et. al. CV 6:10-cv-521-LED Eastern District of Texas*
Engaged on behalf of: Ericsson and Sony Mobile
Technology at Issue: High Speed Data in a 3G Network

Services Provided: Wrote Expert Report on Non-infringement; Gave
Deposition Testimony; Testified at Trial
Law Firm: Thompson Knight
Disposition: Jury finding of no infringement

Year Engaged: 2012

Expert Engagement:
Type of Matter: Patent Investigation
Case Name: *Nazomi Communications, Inc. v Nokia Corp., et al.*
Case No. 5:10-cv-4686-JF 2012 P
Engaged on behalf of: Amazon
Technology at Issue: Android software architecture
Services Provided: Patent Analysis
Law Firm: Greenberg Traurig
Year Engaged: 2012

Expert Engagement:
Type of Matter: Patent Investigation
Case Name: *Summit 6 LLC v Research in Motion, et al*
Case No. cv 3:11-cv-367-O
Engaged on behalf of: Photobucket
Technology at Issue: Multimedia messaging
service ("MMS") messages
Services Provided: Patent Analysis
Law Firm: Fulbright & Jaworski
Year Engaged: 2012

Expert Engagement:
Type of Matter: Patent Investigation
Case Name: *Personal Audio, LLC v. Samsung Electronics Co., Ltd.,*
Case No. cv-432-RC Texas Eastern District
Engaged on behalf of: HTC Corporation
Technology at Issue: Audio playlist functionality
Services Provided: Patent Analysis; Testified at Markman Hearing
Law Firm: Perkins Coie
Year Engaged: 2012

Expert Engagement:
Type of Matter: Patent Investigation
Case Name: *TQP Development, LLC v. Ticketmaster Entertainment, Inc.
et al. Eastern District Texas*
Engaged on behalf of: United Parcel Service
Technology at Issue: Encrypted data transmissions
Services Provided: Patent Analysis
Law Firm: Morris, Manning & Martin
Year Engaged: 2012