

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ARISTA NETWORKS, INC.,
Petitioner,

v.

ORCKIT CORPORATION,
Patent Owner.

Case No. IPR2024-01239
Patent 10,652,111 B2

**DECLARATION OF PAUL MIN, PH.D. IN SUPPORT OF PETITION FOR
INTER PARTES REVIEW OF CLAIMS 1-54 OF
U.S. PATENT NO. 10,652,111 B2**

Table of Contents

	Page
I. INTRODUCTION	10
II. PROFESSIONAL BACKGROUND AND QUALIFICATIONS	11
III. MATERIALS CONSIDERED	17
IV. UNDERSTANDING OF APPLICABLE LEGAL STANDARDS	20
A. My Understanding of Claim Construction	20
B. My Understanding of Obviousness	21
C. Level of Ordinary Skill in the Art	25
V. OVERVIEW OF THE '111 PATENT	26
A. Subject Matter.....	26
B. Prosecution History	31
C. Priority Date.....	33
D. Level of Ordinary Skill in the Art	33
E. Listing of Challenged Claims	34
F. Claim Construction.....	44
1. The “Controller” Term.....	45
2. The “Criterion” Terms	46
VI. TECHNOLOGY BACKGROUND AND STATE OF THE ART	47
A. Deep Packet Inspection	47
B. Software-Defined Networking	50
VII.....APPLICATION OF THE PRIOR ART TO THE CHALLENGED CLAIMS	53
A. Grounds of Unpatentability	54
B. Summary of Prior Art.....	54
1. Overview of Lefebvre (Exhibit 1005).....	54
2. Overview of Chua (Exhibit 1006).....	58
3. Overview of Rash (Exhibit 1007)	59
4. Overview of RFC 793 (Exhibit 1015).....	61

C. Ground 1: Claims 1-6, 9-15, 18-19, 21-36, 41-42, and 44-54 are rendered obvious by Lefebvre in view of Chua	61
1. Motivation to Combine Lefebvre and Chua	62
2. Claim 1	71
(i) 1[Pre]: A method for use with a packet network including a network node for transporting packets between first and second entities under control of a controller that is external to the network node, the method comprising:	
71	
(ii) 1[a]: sending, by the controller to the network node over the packet network, an instruction and a packet-applicable criterion;.....	76
(iii) 1[b]: receiving, by the network node from the controller, the instruction and the criterion;.....	79
(iv) 1[c]: receiving, by the network node from the first entity over the packet network, a packet addressed to the second entity;	80
(v) 1[d]: checking, by the network node, if the packet satisfies the criterion;.....	81
(vi) 1[e]: responsive to the packet not satisfying the criterion, sending, by the network node over the packet network, the packet to the second entity; and	82
(vii) 1[f]: responsive to the packet satisfying the criterion, sending the packet, by the network node over the packet network, to an entity that is included in the instruction and is other than the second entity.	83
3. Claim 2: The method according to claim 1, wherein the instruction is ‘probe’, ‘mirror’, or ‘terminate’ instruction, and upon receiving by the network node the ‘terminate’ instruction, the method further comprising blocking, by the network node, the packet from being sent to the second entity and to the controller.	85
4. Claim 3: The method according to claim 1, wherein the instruction is a ‘probe’, a ‘mirror’, or a ‘terminate’ instruction, and upon receiving by the network node the ‘mirror’ instruction and responsive to the packet satisfying the criterion, the method further comprising sending the packet, by the network node, to the second entity and to the controller.	88
5. Claim 4: The method according to claim 1, wherein the instruction is ‘probe’, ‘mirror’, or ‘terminate’ instruction, and upon receiving by the network node the ‘probe’ instruction and responsive to the packet satisfying the criterion, the method further comprising: sending the packet, by the network	

node, to the controller; responsive to receiving the packet, analyzing the packet, by the controller; sending the packet, by the controller, to the network node; and responsive to receiving the packet, sending the packet, by the network node, to the second entity.....	89
6. Claim 5: The method according to claim 1, further comprising responsive to the packet satisfying the criterion and to the instruction, sending the packet or a portion thereof, by the network node, to the controller.	93
7. Claim 6: The method according to claim 5, further comprising storing the received packet or a portion thereof, by the controller, in memory.	94
8. Claim 9: The method according to claim 5, further comprising responsive to receiving the packet, analyzing the packet, by the controller.....	96
9. Claim 10: The method according to claim 9, further for use with an application server that communicates with the controller, wherein the analyzing comprising sending the packet, by the controller, to the application server, and analyzing the packet by the application server.....	97
10. Claim 11: The method according to claim 10, wherein the analyzing further comprising sending the packet after analyzing by the application server to the controller, and sending the packet, after receiving from the controller by the network node, to the second entity.....	99
11. Claim 12: The method according to claim 9, wherein the analyzing comprises applying security or data analytic application.	101
12. Claim 13: The method according to claim 9, wherein the analyzing comprises applying security application that comprises firewall or intrusion detection functionality.....	103
13. Claim 14: The method according to claim 9, wherein the analyzing comprises performing Deep Packet Inspection (DPI) or using a DPI engine on the packet.....	103
14. Claim 15: The method according to claim 9, wherein the packet comprises distinct header and payload fields, and wherein the analyzing comprises checking part of, or whole of, the payload field.	104
15. Claim 18: The method according to claim 1, wherein the packet comprises distinct header and payload fields, the header comprises at least the first and second entities addresses in the packet network, and wherein the packet-applicable criterion is that the first entity address, the second entity address, or both match a predetermined address or addresses.	106

16. Claim 19: The method according to claim 18, wherein the addresses are Internet Protocol (IP) addresses.	107
17. Claim 21: The method according to claim 1, wherein the packet network comprises a Wide Area Network (WAN), Local Area Network (LAN), the Internet, Metropolitan Area Network (MAN), Internet Service Provider (ISP) backbone, datacenter network, or inter-datacenter network.	108
18. Claim 22: The method according to claim 1, wherein the first entity is a server device and the second entity is a client device, or wherein the first entity is a client device and the second entity is a server device.	109
19. Claim 23: The method according to claim 22, wherein the server device comprises a web server, and wherein the client device comprises a smartphone, a tablet computer, a personal computer, a laptop computer, or a wearable computing device.	111
20. Claim 24: The method according to claim 22, wherein the communication between the network node and the controller is based on, or uses, a standard protocol.	112
21. Claim 25: The method according to claim 24, wherein the standard protocol is according to, based on, or compatible with, an OpenFlow protocol version 1.3.3 or 1.4.0.	113
22. Claim 26: The method according to claim 25, wherein the instruction comprises a Type-Length-Value (TLV) structure.	114
23. Claim 27: The method according to claim 1, wherein the network node comprises a router, a switch, or a bridge.	114
24. Claim 28: The method according to claim 1, wherein the packet network is an Internet Protocol (IP) network, and the packet is an IP packet.	116
25. Claim 29: The method according to claim 28, wherein the packet network is an Transmission Control Protocol (TCP) network, and the packet is an TCP packet.	116
26. Claim 30: The method according to claim 1, further comprising: receiving, by the network node from the first entity over the packet network, one or more additional packets; checking, by the network node, if any one of the one or more additional packets satisfies the criterion; responsive to an additional packet not satisfying the criterion, sending, by the network node over the packet network, the additional packet to the second entity; and responsive to the additional packet satisfying the criterion, sending the additional packet, by the network node over the packet network, in response to the instruction.	117

27. Claim 31: The method according to claim 1, wherein the packet network is a Software Defined Network (SDN), the packet is routed as part of a data plane and the network node communication with the controller serves as a control plane.....	118
28. Claim 32	119
(i) 32[pre]: A method for use with a packet network including a network node for transporting packets between first and second entities under control of a controller that is external to the network node, the method by the network node comprising:	119
(ii) 32[a]: receiving, from the controller, the instruction and the criterion; 120	
(iii) 32[b]: receiving, from the first entity over the packet network, a packet addressed to the second entity;.....	120
(iv) 32[c]: checking if the packet satisfies the criterion;	120
(v) 32[d]: responsive to the packet not satisfying the criterion, sending over the packet network, the packet to the second entity; and	121
(vi) 32[e]: responsive to the packet satisfying the criterion, sending the packet over the packet network, to an entity that is included in the instruction and is other than the second entity.	121
29. Claim 33: The method according to claim 32, wherein the instruction is ‘probe’, ‘mirror’, or ‘terminate’ instruction, and upon receiving the ‘terminate’ instruction, the method further comprising blocking, the packet from being sent to the second entity and to the controller.....	122
30. Claim 34: The method according to claim 32, wherein the instruction is a ‘probe’, a ‘mirror’, or a ‘terminate’ instruction, and upon receiving the ‘mirror’ instruction and responsive to the packet satisfying the criterion, the method further comprising sending the packet to the second entity and to the controller.	122
31. Claim 35: The method according to claim 32, wherein the instruction is ‘probe’, ‘mirror’, or ‘terminate’ instruction, and upon receiving the ‘probe’ instruction and responsive to the packet satisfying the criterion, the method further comprising: sending the packet to the controller; receiving the packet, from the controller; and responsive to receiving the packet, sending the packet, to the second entity.....	123

32. Claim 36: The method according to claim 32, further comprising responsive to the packet satisfying the criterion and to the instruction, sending the packet or a portion thereof to the controller.....	123
33. Claim 41: The method according to claim 32, wherein the packet comprises distinct header and payload fields, the header comprises at least the first and second entities addresses in the packet network, and wherein the packet-applicable criterion is that the first entity address, the second entity address, or both match a predetermined address or addresses.....	123
34. Claim 42: The method according to claim 41, wherein the addresses are Internet Protocol (IP) addresses.	124
35. Claim 44: The method according to claim 32, wherein the packet network comprises a Wide Area Network (WAN), Local Area Network (LAN), the Internet, Metropolitan Area Network (MAN), Internet Service Provider (ISP) backbone, datacenter network, or inter-datacenter network.	124
36. Claim 45: The method according to claim 32, wherein the first entity is a server device and the second entity is a client device, or wherein the first entity is a client device and the second entity is a server device.	124
37. Claim 46: The method according to claim 45, wherein the server device comprises a web server, and wherein the client device comprises a smartphone, a tablet computer, a personal computer, a laptop computer, or a wearable computing device.....	125
38. Claim 47: The method according to claim 45, wherein the communication with the controller is based on, or uses, a standard protocol.	125
39. Claim 48: The method according to claim 47, wherein the standard protocol is according to, based on, or compatible with, an OpenFlow protocol version 1.3.3 or 1.4.0.....	125
40. Claim 49: The method according to claim 48, wherein the instruction comprises a Type-Length-Value (TLV) structure.	126
41. Claim 50: The method according to claim 32, wherein the network node comprises a router, a switch, or a bridge.	126
42. Claim 51: The method according to claim 32, wherein the packet network is an Internet Protocol (IP) network, and the packet is an IP packet.	126
43. Claim 52: The method according to claim 51, wherein the packet network is a Transmission Control Protocol (TCP) network, and the packet is an TCP packet.	127

44. Claim 53: The method according to claim 32, further comprising: receiving, from the first entity over the packet network, one or more additional packets; checking, if any one of the one or more additional packets satisfies the criterion; responsive to an additional packet not satisfying the criterion, sending over the packet network, the additional packet to the second entity; and responsive to the additional packet satisfying the criterion, sending the additional packet over the packet network, in response to the instruction.	127
45. Claim 54: The method according to claim 32, wherein the packet network is a Software Defined Network (SDN), the packet is routed as part of a data plane and the communication with the controller serves as a control plane. .	127
D. Ground 2: Claims 7, 8, 37, and 38 are rendered obvious by Lefebvre in view of Chua and Rash.....	128
1. Motivation to Combine Lefebvre, Chua, and Rash	129
2. Claim 7: The method according to claim 5, further comprising responsive to the packet satisfying the criterion and to the instruction, sending a portion of the packet, by the network node, to the controller.....	134
3. Claim 8: The method according to claim 7, wherein the portion of the packet consists of multiple consecutive bytes, and wherein the instruction comprises identification of the consecutive bytes in the packet.....	135
4. Claim 37: The method according to claim 36, further comprising responsive to the packet satisfying the criterion and to the instruction, sending a portion of the packet to the controller.	136
5. Claim 38: The method according to claim 37, wherein the portion of the packet consists of multiple consecutive bytes, and wherein the instruction comprises identification of the consecutive bytes in the packet.....	136
E. Ground 3: Claims 16-20 and 39-43 are rendered obvious by Lefebvre in view of Chua and RFC 793	136
1. Motivation to Combine RFC 793 with Lefebvre and Chua.....	137
2. Claim 16: The method according to claim 1, wherein the packet comprises distinct header and payload fields, the header comprises one or more flag bits, and wherein the packet-applicable criterion is that one or more of the flag bits is set.....	138
3. Claim 17: The method according to claim 16, wherein the packet is an Transmission Control Protocol (TCP) packet, and wherein the one or more flag bits comprises comprise a SYN flag bit, an ACK flag bit, a FIN flag bit, a RST flag bit, or any combination hereof.	142

4. Claim 18: The method according to claim 1, wherein the packet comprises distinct header and payload fields, the header comprises at least the first and second entities addresses in the packet network, and wherein the packet-applicable criterion is that the first entity address, the second entity address, or both match a predetermined address or addresses.	143
5. Claim 19: The method according to claim 18, wherein the addresses are Internet Protocol (IP) addresses.	144
6. Claim 20: The method according to claim 1, wherein the packet is an Transmission Control Protocol (TCP) packet that comprises source and destination TCP ports, a TCP sequence number, and a TCP sequence mask fields, and wherein the packet-applicable criterion is that the source TCP port, the destination TCP port, the TCP sequence number, the TCP sequence mask, or any combination thereof, matches a predetermined value or values.....	144
7. Claim 39: The method according to claim 32, wherein the packet comprises distinct header and payload fields, the header comprises one or more flag bits, and wherein the packet-applicable criterion is that one or more of the flag bits is set.	148
8. Claim 40: The method according to claim 39, wherein the packet is an Transmission Control Protocol (TCP) packet, and wherein the one or more flag bits comprises comprise a SYN flag bit, an ACK flag bit, a FIN flag bit, a RST flag bit, or any combination thereof.	148
9. Claim 41: The method according to claim 32, wherein the packet comprises distinct header and payload fields, the header comprises at least the first and second entities addresses in the packet network, and wherein the packet-applicable criterion is that the first entity address, the second entity address, or both match a predetermined address or addresses.....	149
10. Claim 42: The method according to claim 41, wherein the addresses are Internet Protocol (IP) addresses.	149
11. Claim 43: The method according to claim 32, wherein the packet is an Transmission Control Protocol (TCP) packet that comprises source and destination TCP ports, a TCP sequence number, and a TCP sequence mask fields, and wherein the packet-applicable criterion is that the source TCP port, the destination TCP port, the TCP sequence number, the TCP sequence mask, or any combination thereof, matches a predetermined value or values.....	150
VIII. SECONDARY CONSIDERATIONS.....	150
IX. CONCLUSION.....	151

I, Paul Min, Ph.D., declare as follows:

I. INTRODUCTION

1. I have been retained by counsel for Arista Networks, Inc. (the “Petitioner”) in connection with the above-captioned *inter partes* review (“IPR”) of Claims 1-54 of U.S. Patent No. 10,652,111 B2 (the “’111 Patent”), entitled Method And System For Deep Packet Inspection In Software Defined Networks, by named inventors Yossi Barsheshet, Simhon Doctori, and Ronen Solomon. I understand that the ’111 Patent is assigned to Orckit Corporation (the “Patent Owner”). I have been asked to provide technical review, analysis, insights, and opinions regarding the ’111 Patent and the prior art references that form the basis for the grounds of unpatentability set forth in the Petition for *Inter Partes* Review of the ’111 Patent (the “Petition”). I have been asked to provide a declaration regarding my opinions on the validity of Claims 1-54 of the ’111 Patent.

2. This declaration sets forth the opinions I have formed in this IPR and provides the bases and reasons for those opinions. I have summarized in this section my educational background, professional experience, and publications. My education and professional experience are described in my curriculum vita, attached to this declaration as Appendix A.

3. This declaration is based on information currently available to me. I declare that I have personal knowledge of the facts set forth in this declaration and, if called to testify as a witness, could and would do so competently.

4. I am being compensated at my usual consulting rate of \$500 per hour for my work on this matter. I am also being reimbursed for any incurred expenses. My compensation is in no way dependent upon my opinions or testimony or the outcome of this proceeding. I have no other interests in this proceeding or with Petitioner or Patent Owner.

II. PROFESSIONAL BACKGROUND AND QUALIFICATIONS

5. A description of my professional background and qualifications is provided below. An additional account of my work experience and qualifications is included in my curriculum vitae, which is attached as Appendix A.

6. I am an expert in the field of high speed communication and computing, and the development of electronic devices and software systems and for the related applications. I am currently a Senior Professor in the Department of Electrical and Systems Engineering at Washington University in Saint Louis.

7. I received a B.S. degree in Electrical Engineering in 1982, an M.S. degree in Electrical Engineering in 1984, and a Ph.D. degree in Electrical Engineering in 1987 from the University of Michigan in Ann Arbor. I received several academic honors, including my B.S. degree with honors, a best graduate

student award and a best teaching assistant award during my M.S. study, and a best paper award from a major international conference for reporting results from my Ph.D. thesis.

8. After receiving my Ph.D., I worked at Bellcore in New Jersey from August 1987 until August 1990. At Bellcore, I was responsible for evolving the public switched telephone network (PSTN) into a multi-services voice and data network that incorporated packet switches, optical technologies, and wireless technologies. I received an Outstanding Achievement Award for my contributions to Bellcore in 1989.

9. In September 1990, I joined the faculty at Washington University in St. Louis. Upon arriving at Washington University, I developed a communication and computer curricula in the School of Engineering and Applied Science. I regularly teach undergraduate and graduate courses. In July 1996, I was promoted to an Associate Professor of Electrical Engineering with tenure. I am currently a Senior Professor of Electrical and Systems Engineering at Washington University. I have served as the Chair of the Graduate Curriculum (2000–2002) and the Chair of the Undergraduate Curriculum (2011–2014) for the Department of Electrical and Systems Engineering.

10. At Washington University, I have conducted research in communication, computing, and related electronic hardware and software. My

research group has pioneered a new paradigm for computing and communication systems that can alleviate the speed and performance mismatch against optical technology. I have received several grants from U.S. Federal Agencies, including the National Science Foundation (NSF), the Defense Advanced Research Project Agency (DARPA), and the Air Force Office of Scientific Research (AFOSR), and numerous contracts from companies and organizations around the world.

11. My research group has significantly contributed to development of future generations of wireless technology. I developed methods that enable coordinated transmission and reception of wireless signals among multiple base stations. Previously, radio signals from multiple base stations were considered as interference. Leveraging my research, a cluster of base stations can work together as a single resource enhancing the quality of radio signals across extremely noisy wireless channels.

12. I developed and implemented a number of semiconductor integrated circuit chips. These integrated circuit chips include switch fabrics, processors, high speed interfaces, protocol transposers, controllers, content search engines, look up table processors, and memory cells and arrays.

13. Specifically related to the technology matters in this litigation, I have researched a variety of technologies for the packet switches and routers including packet scheduler, traffic shaper, traffic policing, buffer management, and interposer.

In addition, I have researched and implemented various look-up table configurations for fast packet processing, which is particularly applicable to the Multi Protocol Lable Switching or MPLS. Moreover, since the mid 1990s, I have been researching and developing various security technologies such as deep packet inspection, content searching and matching, regular expression processing, etc.

14. As a faculty member at Washington University, I have taught a number of courses in electronics, communication, and computing at both the undergraduate and graduate levels. For example, I have taught Communication Theory (Washington University ESE 471), Transmission and Multiplexing (Washington University ESE 571), and Signaling and Control of Communication Networks (Washington University ESE 572).

15. I have directly supervised numerous graduate students, a number of whom received a doctoral degree under my guidance. A number of doctoral theses that I have supervised relate specifically to the aforementioned-communication and computing technologies related to this litigation. My students and I have published a number of peer-reviewed articles in these topics.

16. In addition to my responsibilities as a university faculty member, I have founded two companies. In May 1997, I founded MinMax Technologies, Inc., a fabless semiconductor company that developed switch fabric integrated circuit chips for the Internet. In March 1999, I founded Erlang Technology, Inc., a fabless

semiconductor company that focused on the design and development of integrated circuit chips and software for the Internet. One of Erlang's products received a best product of the year award in 2004 from a major trade journal for the electronics industry.

17. Outside my own start-up companies, I have also served in various technology and business advisor roles for other companies and organizations around the world. I was the main technical author for one of two winning proposals to the Korean government for CDMA wireless service licenses (1996). I was responsible for designing a commercial scale IS-95 CDMA cellular network, which I understand to be one of the earliest such networks deployed in the world. I worked with numerous engineers and scientists around the world to implement this commercial-scale cellular network before IS-95 CDMA was widely accepted. This provided me with extensive insight into various components of commercial-scale communication technology used today. I have also been involved in a semiconductor company that specializes in semiconductor memories, such as flash EEPROMs, as a board member and as a technical advisor (2007–2011).

18. I am a named inventor on eleven U.S. patents. I have authored and co-authored numerous technical papers and memoranda, many of which have appeared in various peer-reviewed international journals and conferences. I have given more

than 100 seminars and invited talks around the world. I have organized several international conferences and served as an international journal editor.

19. I am a member of, and have been actively involved in, a number of professional organizations. I have served as the Chair of the St. Louis Section of the IEEE, which has more than 3,000 members (2014), and a member of the Eta Kappa Nu Honor Society for electrical engineers. I have also been an Ambassador of the McDonnell International Scholars Academy (2007–2013).

20. I was a member of the Presidential Business Advisors Committee (to President George W. Bush) and was named 2002 Businessman of the Year by the Wall Street Journal for the State of Missouri, for my entrepreneurial efforts.

21. I have received multiple awards for my publications and contributions to technical communication systems. In 1988, I received the Best Paper Award at 18th ISATA Award of Technical Excellence in Florence, Italy. I was also a Rockwell Fellow at the University of Michigan in Ann Arbor in 1988 and 1989. I received a Research Initiation Award in 1993 from the Defense Advance Research Project Agency (DARPA). I received the Best Paper Award at MOBILITY 2011 in Barcelona, Spain. In my more than 30 years of experience with telecommunications technology, I have acquired significant knowledge about telecommunications systems industry standards and standard setting organizations such as ANSI, IEEE, ITU, IETF, and 3GPP.

22. Additional details of my education and work experience, awards and honors, and publications that may be relevant to the opinions I have formed are set forth in my curriculum vitae. *See* Appendix A. A list of cases in which I have testified as an expert at trial or by deposition is included in Appendix A.

III. MATERIALS CONSIDERED

23. The analysis that I provide in this declaration is based on my education, research, experience, and professional judgment, as well as the documents I have considered, including the '111 Patent (Exhibit 1001) and its prosecution history (Exhibit 1003). I have reviewed and am familiar with the specification of the '111 Patent. I have reviewed and am familiar with the file history of the '111 Patent.

24. In preparing this declaration, I have also reviewed and am familiar with the following prior art used in the Petition and in my declaration below:¹

¹ The '111 Patent claims priority to U.S. Provisional Application No. 61/982,358 filed on April 22, 2014. For purposes of this declaration, I have been asked to assume that the priority date for the '111 Patent is April 22, 2014, the date the provisional application was filed. I do not offer an opinion on whether the '111 Patent is in fact entitled to claim the benefit of the filing date of the provisional application.

Exhibit 1005 – U.S. Patent No. 10,097,452 B2 by Lefebvre (“Lefebvre”) was filed on July 24, 2012, which is before the assumed April 22, 2014 priority date of the ’111 Patent. I understand from counsel for Petitioner that Lefebvre qualifies as prior art under at least AIA 35 U.S.C. § 102(a)(2).

Exhibit 1006 – U.S. Patent No. 9,264,301 B1 by Chua (“Chua”) was filed on March 15, 2013, which is before the assumed April 22, 2014 priority date of the ’111 Patent. I understand from counsel for Petitioner that Chua qualifies as prior art under at least AIA 35 U.S.C. § 102(a)(2).

Exhibit 1007 – U.S. Patent No. 9,813,447 by Rash (“Rash”) was filed on March 15, 2013, which is before the assumed April 22, 2014 priority date of the ’111 Patent. I understand from counsel for Petitioner that Rash qualifies as prior art under at least AIA 35 U.S.C. § 102(a)(2).

Exhibit 1015 – RFC: 793, Transmission Control Protocol, DARPA Internet Program Protocol Specification (“RFC 793”) was published September 1981. I understand from counsel for Petitioner that RFC 793 qualifies as prior art under at least AIA 35 U.S.C. § 102(a)(1).

25. I have considered the following documents in my analysis below:

Exhibit No.	Description
1001	U.S. Patent No. 10,652,111 (“’111 Patent”)
1003	Prosecution File History of the ’111 Patent
1005	U.S. Patent No. 10,097,452 (“Lefebvre”)
1006	U.S. Patent No. 9,264,301 (“Chua”)

Exhibit No.	Description
1007	U.S. Patent No. 9,813,447 (“Rash”)
1008	M. Liao, <i>et al.</i> , “Design and Evaluation of Deep Packet Inspection System: A Case Study,” IET Networks, pp. 1-8 (2012) (“Liao”)
1009	A. W. Moore and K. Papagiannaki, “Toward the Accurate Identification of Network Applications,” In: PAM, Springer, vol. 5, pp. 41-54 (2005) (“Moore”)
1010	RFC 3654 (available at https://www.rfc-editor.org/rfc/rfc3654)
1011	W. Xia, <i>et al.</i> , “A Survey on Software-Defined Networking,” IEEE Communication Surveys & Tutorials, Vol. 17, No. 1, pp. 27-51 (June 13, 2014) (“Xia”)
1012	RFC 3746 (available at https://www.rfc-editor.org/in-notes/rfc3746.txt)
1013	N. McKeown, <i>et al.</i> , “OpenFlow: Enabling Innovation in Campus Networks,” ACM SIGCOMM Computer Communication Review, vol. 38, No. 2, pp. 69-74 (April 2008) (“McKeown”)
1014	Steven Levy, “Going with the Flow: Google’s Secret Switch to the Next Wave of Networking” (April 17, 2012) (available at https://www.wired.com/2012/04/going-with-the-flow-google/)
1015	RFC 793 (available at https://www.rfc-editor.org/rfc/pdf/rfc793.txt.pdf)
1016	“About the Open Networking Foundation”
1017	“Open Networking Foundation Specifications,” (available at https://opennetworking.org/software-defined-standards/specifications/)
1018	“OpenFlow Switch Specification”
1019	RFC 5810 (available at https://www.rfc-editor.org/rfc/rfc5810.html)
1025	RFC 2026
1026	U.S. Patent Application Publication No. 2007/0094411 by Mullane (April 26, 2007)
1027	OpenFlow Switch Specification, Version 1.1.0 (available at https://opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.1.0.pdf)

26. In reaching the opinions expressed in this declaration, I have also considered the Declaration Of Dr. Nader F. Mir Under 37 C.F.R. § 1.68 In Support

Of Petition for *Inter Partes* Review submitted as Exhibit 1003 in IPR2024-00895. Although this declaration is not identical to Dr. Mir's, and addresses claims not expressly considered in Dr. Mir's declaration, I have in places repeated portions of Dr. Mir's analysis in this declaration. Where I have repeated or otherwise relied on Dr. Mir's analysis, I agree with Dr. Mir's analysis and adopt it as my own for purposes of this declaration.

IV. UNDERSTANDING OF APPLICABLE LEGAL STANDARDS

27. Although I am not an attorney, I have a general understanding of the applicable legal standards pertaining to the patentability issues presented in this proceeding. My understanding of legal principles as described in this section is based on communication of those principles to me by Petitioner's legal counsel. The analysis in this declaration is in accordance with the legal principles outlined below.

28. I understand that, in this *inter partes* review, Petitioner has the burden of proving that each challenged claim is unpatentable by a preponderance of the evidence.

A. My Understanding of Claim Construction

29. I have been informed by counsel that a purpose of claim construction is to determine what a person of ordinary skill in the art ("POSITA") would have understood the claim terms to mean. I understand that during an IPR proceeding, claims are to be construed in light of the specification as would be read by a POSITA

at the time the application was filed. I understand that claim terms are given their ordinary and customary meaning as would be understood by a POSITA in the context of the entire disclosure. A claim term, however, will not receive its ordinary meaning if the patentee acted as his own lexicographer and clearly set forth a definition of the claim term in the specification. In this case, the claim term will receive the definition set forth in the patent.

30. I understand that the prosecution history can inform the meaning of the claim language by demonstrating how the inventors understood the invention and whether the inventors limited the invention in the course of prosecution, making the claim scope narrower than it otherwise would be. I understand that extrinsic evidence may also be consulted in construing the claim terms, such as dictionary definitions and expert testimony.

B. My Understanding of Obviousness

31. I understand that a patent claim is unpatentable if, at the time of the invention, it would have been obvious to one of ordinary skill in the art to combine the teachings of the prior art to yield the patent claim. I also understand that it is not required (although it is acceptable) that each element of a patent claim be found in a single reference in order to find a patent claim obvious. This means that even if all of the requirements of the claim cannot be found in a single prior art reference that would anticipate the claim, the claim can still be invalid. For a patent claim to be

found obvious, all the elements of the patent claim may be found in a combination of references at which a POSITA would have been reasonable expected to arrive.

32. I understand that the following factors should be considered in analyzing obviousness: (1) the scope and content of the prior art; (2) the differences between the prior art and the claims; (3) the level of ordinary skill in the pertinent art; and (4) other objective considerations identified below. I understand that an invention is obvious when the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a POSITA at the time the invention was made.

33. I understand that a showing of obviousness requires some articulated reasoning with a rational underpinning to support the combination of references. I understand that in consideration of the issue of obviousness it is important to identify whether a reason existed at the time of the invention that would have led a person of ordinary skill in the pertinent art to combine elements of the references in a way that yields the claimed invention.

34. I understand that a POSITA is assumed to have knowledge of all prior art references. I also understand that when considering the obviousness of a patent claim, one may consider whether a teaching, suggestion, or motivation to combine the references exists so as to avoid impermissibly applying hindsight when considering the prior art.

35. I understand that a POSITA can combine various prior art references based on the teachings of those prior art references, the general knowledge present in the art, or common sense. I understand that a motivation to combine the references may be implicit in the prior art, and there is no requirement that there be an actual or explicit teaching to combine two references. Thus, one may take into account the inferences and creative steps that a POSITA would employ to combine the known elements in the prior art in the manner claimed by the patent-at-issue. I understand that one should avoid “hindsight bias” and ex post reasoning in performing an obviousness analysis. This does not mean, however, that a POSITA does not have recourse to common sense for purposes of the obviousness inquiry.

36. I understand that a claim may be considered unpatentable for obviousness for various reasons. I have been informed that the following exemplary rationales may support a finding of obviousness:

- A) combining prior art elements according to known methods to yield predictable results;
- B) simply substituting one known element for another to obtain predictable results;
- C) use of a known technique to improve similar devices (methods, or products) in the same way;

- D) applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
- E) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success;
- F) a predictable variation of work in the same or a different field of endeavor, which a POSITA would be able to implement;
- G) if, at the time of the alleged invention, there existed a known problem for which there was an obvious solution encompassed by the patent's claim;
- H) known work in one field of endeavor that prompts variations of it for use in either the same field or a different field based on technological incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; and/or
- I) some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior-art reference or to combine multiple prior-art references or teachings to arrive at the claimed invention.

37. I understand that even if a prima facie case of obviousness is established, the final determination of obviousness must also consider objective indicia of nonobviousness, which I understand are also referred to as “secondary considerations,” if presented. I understand that these objective indicia can be important evidence as to whether a patent is obvious or nonobvious. Such secondary

considerations include: (1) commercial success of products covered by the patent claims; (2) a long-felt but unsolved need for the invention; (3) failed attempts by others to make the invention; (4) copying of the invention by others in the field; (5) unexpected results achieved by the invention as compared to the closest prior art; (6) praise of the invention by the infringer or others in the field; (7) the taking of licenses under the patent by others; (8) expressions of surprise by experts and those skilled in the art at the making of the invention; and (9) the patentee proceeded contrary to the accepted wisdom of the prior art. I further understand that secondary considerations evidence is only relevant if the offering party establishes a connection, or nexus, between the evidence and the claimed invention.

C. Level of Ordinary Skill in the Art

38. I understand that an assessment of the claims of the '111 Patent should be undertaken from the perspective of a POSITA as of the earliest claimed priority date. I understand that a POSITA is presumed to be aware of all pertinent art, thinks along conventional wisdom in the art, and is a person of ordinary creativity—not an automaton.

39. I understand that to determine the appropriate level of a POSITA, the following factors may be considered: (1) the types of problems encountered by those working in the field and prior art solutions thereto; (2) the sophistication of the technology in question, and the rapidity with which innovations occur in the field;

(3) the educational level of active workers in the field; and (4) the educational level of the inventor.

V. OVERVIEW OF THE '111 PATENT

40. I have reviewed the '111 Patent, which is entitled “Method and System for Deep Packet Inspection in Software Defined Networks.” EX1001 (“'111 Patent”) at Cover. I understand that the '111 Patent claims priority to a provisional application filed on April 22, 2014.

A. Subject Matter

41. The '111 Patent is titled “Method and System for Deep Packet Inspection in Software Defined Networks.” The cover shows the applicants filed a U.S. provisional application on April 22, 2014, and filed the corresponding international application on April 21, 2015.

42. The '111 Patent describes a method for deep packet inspection (DPI) in a software defined network (SDN) where “the method is performed by a central controller of the SDN.” *See, e.g.*, '111 Patent at 2:27-30, 2:50-51, 4:5-7 (“The central controller 111 is configured to perform deep packet inspection on designated packets from designated flows or TCP sessions.”). Specifically, the controller 111 instructs network nodes 112 to determine if incoming packets from client devices 130 communicating with destination servers 140 require inspection. '111 Patent at 4:8-11, FIG. 6 (step S610). The controller 111 and the network nodes 112

communicate using standard protocols such as OpenFlow. '111 Patent at 3:44-48. The network nodes 112 redirect or mirror packets for inspection by the controller 111. '111 Patent at 4:15-18. The controller 111 then provides inspected data to application servers 120 for further processing associated with security applications, for example. '111 Patent at 3:56-61.

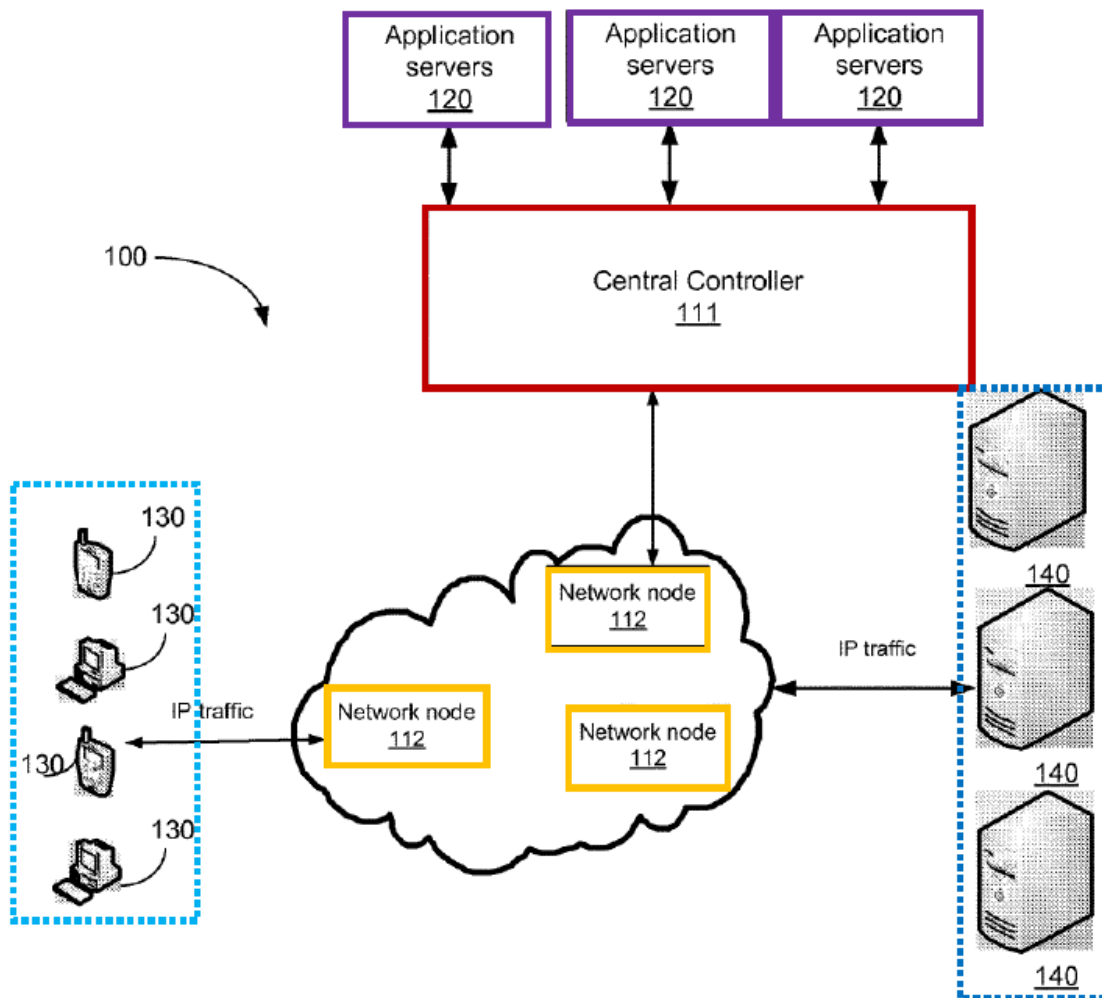
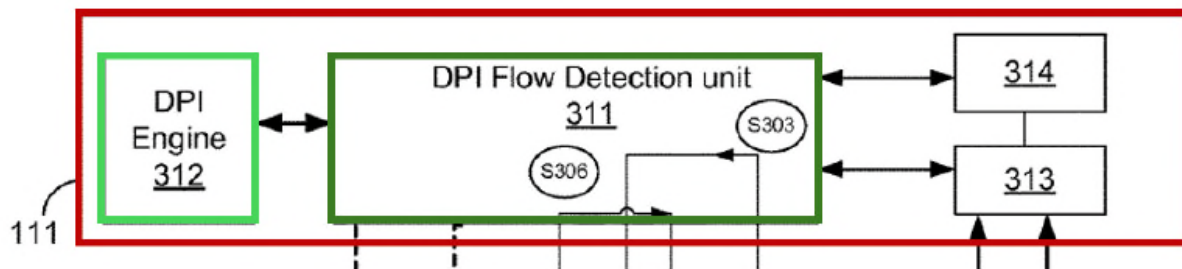


FIG. 1

'111 Patent at FIG. 1 (annotated).

43. The controller 111 includes memory 313 and processing unit 314. '111 Patent at 5:33-36. Similarly, network nodes 112 each include memory 322 and processing unit 323. '111 Patent at 5:50-52. The processing unit 314 of controller 111 executes “tasks generally performed by the central controllers of SDN.” '111 Patent at 5:60-64. The controller 111 also includes components such as the DPI flow detection module 311 and DPI engine 312. '111 Patent at 5:30-39. And similarly, the network nodes 112 each also include a probe flow module 321. '111 Patent at 5:50-59.



'111 Patent at FIG. 1 (annotated).

44. To perform the '111 Patent's DPI method, the controller 111 provides instructions to the network nodes 112. '111 Patent at 6:10-12, 9:40-46, FIG. 6 (step S610). In an embodiment disclosed by the '111 Patent, when the instructions apply to a packet, the probe flow module 321 of the network nodes 112 redirects the packet to the DPI flow detection module 311 of the controller 111. '111 Patent at 5:50-59, 6:12-19, 6:27-32, 6:41-52, 9:47-61, FIG. 6. The DPI flow detection module 311 then executes steps including trapping the packet, creating a new entry in the flow

table, and providing the packet for analysis by the DPI engine 312. '111 Patent at 6:20-26, 6:33-40, 6:41-52, 8:1-14. The DPI flow detection module 311 may also update the instructions for network nodes 112. '111 Patent at 7:54-56 (“In an embodiment, a set of mirroring instructions generated respective of the computed mask value are sent to the node 112.”), 9:62-10:3, FIG. 6 (step S650). And after inspection, the DPI engine 312 of the controller 111 may provide application metadata to the application servers 120. '111 Patent at 5:36-39. The '111 Patent discloses that implementation of its embodiments as “hardware, firmware, software, or any combination” is possible. '111 Patent at 10:15-36.

45. Independent claim 1, which recites a method for use with a packet network including a network node for transporting packets between first and second entities under control of a controller that is external to the network node, is reproduced below:

1. A method for use with a packet network including a network node for transporting packets between first and second entities under control of a controller that is external to the network node, the method comprising:

sending, by the controller to the network node over the packet network, an instruction and a packet-applicable criterion;

receiving, by the network node from the controller, the instruction and the criterion;

receiving, by the network node from the first entity over the packet network, a packet addressed to the second entity;

checking, by the network node, if the packet satisfies the criterion;

responsive to the packet not satisfying the criterion, sending, by the network node over the packet network, the packet to the second entity; and

responsive to the packet satisfying the criterion, sending the packet, by the network node over the packet network, to an entity that is included in the instruction and is other than the second entity.

'111 Patent at 10:52-11:4. Claims 2-31 depend, directly or indirectly, from claim 1.

46. Independent Claim 32, the only other independent claim in the '111 Patent, similarly recites a method for use with a packet network including a network node for transporting packets between first and second entities under control of a controller that is external to the network node. Claim 32 is reproduced below.

32. A method for use with a packet network including a network node for transporting packets between first and second entities under control

of a controller that is external to the network node, the method by the network node comprising:

receiving, from the controller, the instruction and the criterion;

receiving, from the first entity over the packet network, a packet addressed to the second entity;

checking if the packet satisfies the criterion;

responsive to the packet not satisfying the criterion, sending over the packet network, the packet to the second entity; and

responsive to the packet satisfying the criterion, sending the packet over the packet network, to an entity that is included in the instruction and is other than the second entity.

'111 Patent at 13:8-23.

B. Prosecution History

47. On April 22, 2014, the applicant filed U.S. Provisional Application No. 61/982,358 which contained ten pages of figures and descriptions. '111 Patent at Cover (INID code (60)); EX1003, 130-146. The applicant filed an International Application on April 21, 2015 that designated the United States, among other countries. EX1003, 5 (INID codes (22), (81)). And the application entered the U.S. National Stage on September 15, 2016. '111 Patent at Cover (INID code (86)).

Upon entry, the applicant presented 54 claims. EX1003, 54-63 (claims of the 09/15/2016 Preliminary Amendment).

48. The Examiner rejected all 54 claims as being unpatentable over U.S. Patent Application Publication No. 2010/0208590 (“Dolganow”) and U.S. Patent Application Publication No. 2014/0052836 (“Nguyen”). EX1003, 271-296 (09/12/2018 Office Action). The applicant argued against the rejections in its Response. EX1003, 322-330 (12/10/2018 Response). The Examiner issued a Final Rejection relying on the same unpatentability grounds. EX1003, 331-357 (04/15/2019 Office Action). The applicant then amended the independent claims to recite that the controller was “external to the network node” and that the packets satisfying the criterion were sent “to an entity that is included in the instruction and is other than the second entity.” EX1003, 397-417 (05/07/2019 Amendment).

49. In the next Office Action, the Examiner rejected all 54 claims as being unpatentable over Dolganow and U.S. Patent Application Publication No. 2016/0219080 (“Huang”). EX1003, 425-451 (07/08/2019 Office Action). The applicant argued against the rejections in its Response. EX1003, 492-501 (10/02/2019 Response). The Examiner issued a Notice of Allowance on January 7, 2020, stating that the claims were allowed for the reasons the applicant argued. EX1003, 504-510 (01/07/2020 Notice of Allowance). The ’111 Patent issued on May 12, 2020. ’111 Patent at Cover (code (10)).

C. Priority Date

50. For purposes of this declaration, I have been asked to assume that the '111 Patent is entitled to a priority date of April 22, 2014, the filing date of U.S. Provisional Application No. 61/982,358. I have not considered whether the '111 Patent is in fact entitled to the benefit of the filing date of the provisional application.

D. Level of Ordinary Skill in the Art

51. I have been asked to consider the level of ordinary skill in the field that someone would have had at the time the claimed invention was made. My opinions regarding the level of ordinary skill in the art are based on, among other things, my over 40 years of experience in the field of electrical engineering and computer science, as well as: the levels of education and experience of persons working in the field; the types of problems encountered in the field; and the sophistication of the technology.

52. Based on the disclosure of the '111 Patent, in my opinion a POSITA as of April 22, 2014 would have had at least a Bachelor's degree in computer science, electrical engineering, computer engineering, or a closely related field, and two or more years of professional experience in packet-switched networking systems. Alternatively, a POSITA would have a Master's degree or similar post-graduate work in computer science, electrical engineering, computer engineering, or a closely

related field, and less professional experience. This level of skill is approximate, and more experience would compensate for less formal education, and vice versa.

53. Based on my education and experience, I meet this definition of one of ordinary skill in the art, and I believe that I am qualified to provide opinions about how a POSITA at the relevant time would have interpreted and understood the '111 Patent and the prior art relied upon herein. Although my qualifications and experience exceed those of a POSITA, both in April 2014 and today, I have nevertheless applied the perspective of a POSITA in rendering my opinions below.

54. My opinions below explain how a POSITA would have understood the technology described in the '111 Patent and the prior art references I have identified herein around the April 22, 2014 timeframe. For purposes of this declaration, in general, and unless otherwise noted, my testimony below refers to the knowledge of one of ordinary skill in the art during the time period around the priority date of the '111 Patent. I would have been a person with at least ordinary skill in the art at that time.

E. Listing of Challenged Claims

55. Below I provide a listing of Claims 1-54 of the '111 Patent. I will refer throughout this declaration to the elements of the claims with reference to the number and letter designations that have been added in the left column (e.g., "1[pre]," "1[a]," "1[b]," etc.).

Claim 1	
1[Pre]	A method for use with a packet network including a network node for transporting packets between first and second entities under control of a controller that is external to the network node, the method comprising:
1[a]	sending, by the controller to the network node over the packet network, an instruction and a packet-applicable criterion;
1[b]	receiving, by the network node from the controller, the instruction and the criterion;
1[c]	receiving, by the network node from the first entity over the packet network, a packet addressed to the second entity;
1[d]	checking, by the network node, if the packet satisfies the criterion;
1[e]	responsive to the packet not satisfying the criterion, sending, by the network node over the packet network, the packet to the second entity; and
1[f]	responsive to the packet satisfying the criterion, sending the packet, by the network node over the packet network, to an entity that is included in the instruction and is other than the second entity.
Claim 2	
2	The method according to claim 1, wherein the instruction is ‘probe’, ‘mirror’, or ‘terminate’ instruction, and upon receiving by the network node the ‘terminate’ instruction, the method further comprising blocking, by the network node, the packet from being sent to the second entity and to the controller.
Claim 3	
3	The method according to claim 1, wherein the instruction is a ‘probe’, a ‘mirror’, or a ‘terminate’ instruction, and upon receiving by the network node the ‘mirror’ instruction and responsive to the packet satisfying the criterion, the method further comprising sending the packet, by the network node, to the second entity and to the controller.
Claim 4	

4	The method according to claim 1, wherein the instruction is ‘probe’, ‘mirror’, or ‘terminate’ instruction, and upon receiving by the network node the ‘probe’ instruction and responsive to the packet satisfying the criterion, the method further comprising: sending the packet, by the network node, to the controller; responsive to receiving the packet, analyzing the packet, by the controller; sending the packet, by the controller, to the network node; and responsive to receiving the packet, sending the packet, by the network node, to the second entity.
Claim 5	
5	The method according to claim 1, further comprising responsive to the packet satisfying the criterion and to the instruction, sending the packet or a portion thereof, by the network node, to the controller.
Claim 6	
6	The method according to claim 5, further comprising storing the received packet or a portion thereof, by the controller, in a memory.
Claim 7	
7	The method according to claim 5, further comprising responsive to the packet satisfying the criterion and to the instruction, sending a portion of the packet, by the network node, to the controller.
Claim 8	
8	The method according to claim 7, wherein the portion of the packet consists of multiple consecutive bytes, and wherein the instruction comprises identification of the consecutive bytes in the packet.
Claim 9	
9	The method according to claim 5, further comprising responsive to receiving the packet, analyzing the packet, by the controller.
Claim 10	
10	The method according to claim 9, further for use with an application server that communicates with the controller, wherein the analyzing comprising sending the packet, by the controller, to the application

	server, and analyzing the packet by the application server.
Claim 11	
11	The method according to claim 10, wherein the analyzing further comprising sending the packet after analyzing by the application server to the controller, and sending the packet, after receiving from the controller by the network node, to the second entity.
Claim 12	
12	The method according to claim 9, wherein the analyzing comprises applying security or data analytic application.
Claim 13	
13	The method according to claim 9, wherein the analyzing comprises applying security application that comprises firewall or intrusion detection functionality.
Claim 14	
14	The method according to claim 9, wherein the analyzing comprises performing Deep Packet Inspection (DPI) or using a DPI engine on the packet.
Claim 15	
15	The method according to claim 9, wherein the packet comprises distinct header and payload fields, and wherein the analyzing comprises checking part of, or whole of, the payload field.
Claim 16	
16	The method according to claim 1, wherein the packet comprises distinct header and payload fields, the header comprises one or more flag bits, and wherein the packet-applicable criterion is that one or more of the flag bits is set.
Claim 17	
17	The method according to claim 16, wherein the packet is an Transmission Control Protocol (TCP) packet, and wherein the one or

	more flag bits comprises comprise a SYN flag bit, an ACK flag bit, a FIN flag bit, a RST flag bit, or any combination thereof.
Claim 18	
18	The method according to claim 1, wherein the packet comprises distinct header and payload fields, the header comprises at least the first and second entities addresses in the packet network, and wherein the packet-applicable criterion is that the first entity address, the second entity address, or both match a predetermined address or addresses.
Claim 19	
19	The method according to claim 18, wherein the addresses are Internet Protocol (IP) addresses.
Claim 20	
20	The method according to claim 1, wherein the packet is an Transmission Control Protocol (TCP) packet that comprises source and destination TCP ports, a TCP sequence number, and a TCP sequence mask fields, and wherein the packet-applicable criterion is that the source TCP port, the destination TCP port, the TCP sequence number, the TCP sequence mask, or any combination thereof, matches a predetermined value or values.
Claim 21	
21	The method according to claim 1, wherein the packet network comprises a Wide Area Network (WAN), Local Area Network (LAN), the Internet, Metropolitan Area Network (MAN), Internet Service Provider (ISP) backbone, datacenter network, or inter-datacenter network.
Claim 22	
22	The method according to claim 1, wherein the first entity is a server device and the second entity is a client device, or wherein the first entity is a client device and the second entity is a server device.
Claim 23	
23	The method according to claim 22, wherein the server device comprises

	a web server, and wherein the client device comprises a smartphone, a tablet computer, a personal computer, a laptop computer, or a wearable computing device.
Claim 24	
24	The method according to claim 22, wherein the communication between the network node and the controller is based on, or uses, a standard protocol.
Claim 25	
25	The method according to claim 24, wherein the standard protocol is according to, based on, or compatible with, an OpenFlow protocol version 1.3.3 or 1.4.0.
Claim 26	
26	The method according to claim 25, wherein the instruction comprises a Type-Length-Value (TLV) structure.
Claim 27	
27	The method according to claim 1, wherein the network node comprises a router, a switch, or a bridge.
Claim 28	
28	The method according to claim 1, wherein the packet network is an Internet Protocol (IP) network, and the packet is an IP packet.
Claim 29	
29	The method according to claim 28, wherein the packet network is an Transmission Control Protocol (TCP) network, and the packet is an TCP packet.
Claim 30	
30	The method according to claim 1, further comprising: receiving, by the network node from the first entity over the packet network, one or more additional packets; checking, by the network node, if any one of the one or more additional packets satisfies the criterion; responsive to an

	additional packet not satisfying the criterion, sending, by the network node over the packet network, the additional packet to the second entity; and responsive to the additional packet satisfying the criterion, sending the additional packet, by the network node over the packet network, in response to the instruction.
Claim 31	
31	The method according to claim 1, wherein the packet network is a Software Defined Network (SDN), the packet is routed as part of a data plane and the network node communication with the controller serves as a control plane.
Claim 32	
32[pre]	A method for use with a packet network including a network node for transporting packets between first and second entities under control of a controller that is external to the network node, the method by the network node comprising:
32[a]	receiving, from the controller, the instruction and the criterion;
32[b]	receiving, from the first entity over the packet network, a packet addressed to the second entity;
32[c]	checking if the packet satisfies the criterion;
32[d]	responsive to the packet not satisfying the criterion, sending over the packet network, the packet to the second entity; and
32[e]	responsive to the packet satisfying the criterion, sending the packet over the packet network, to an entity that is included in the instruction and is other than the second entity.
Claim 33	
33	The method according to claim 32, wherein the instruction is ‘probe’, ‘mirror’, or ‘terminate’ instruction, and upon receiving the ‘terminate’ instruction, the method further comprising blocking, the packet from being sent to the second entity and to the controller.
Claim 34	

34	The method according to claim 32, wherein the instruction is a ‘probe’, a ‘mirror’, or a ‘terminate’ instruction, and upon receiving the ‘mirror’ instruction and responsive to the packet satisfying the criterion, the method further comprising sending the packet to the second entity and to the controller.
Claim 35	
35	The method according to claim 32, wherein the instruction is ‘probe’, ‘mirror’, or ‘terminate’ instruction, and upon receiving the ‘probe’ instruction and responsive to the packet satisfying the criterion, the method further comprising: sending the packet to the controller; receiving the packet, from the controller; and responsive to receiving the packet, sending the packet, to the second entity.
Claim 36	
36	The method according to claim 32, further comprising responsive to the packet satisfying the criterion and to the instruction, sending the packet or a portion thereof to the controller.
Claim 37	
37	The method according to claim 36, further comprising responsive to the packet satisfying the criterion and to the instruction, sending a portion of the packet to the controller.
Claim 38	
38	The method according to claim 37, wherein the portion of the packet consists of multiple consecutive bytes, and wherein the instruction comprises identification of the consecutive bytes in the packet.
Claim 39	
39	The method according to claim 32, wherein the packet comprises distinct header and payload fields, the header comprises one or more flag bits, and wherein the packet-applicable criterion is that one or more of the flag bits is set.
Claim 40	

40	The method according to claim 39, wherein the packet is an Transmission Control Protocol (TCP) packet, and wherein the one or more flag bits comprises comprise a SYN flag bit, an ACK flag bit, a FIN flag bit, a RST flag bit, or any combination thereof.
Claim 41	
41	The method according to claim 32, wherein the packet comprises distinct header and payload fields, the header comprises at least the first and second entities addresses in the packet network, and wherein the packet-applicable criterion is that the first entity address, the second entity address, or both match a predetermined address or addresses.
Claim 42	
42	The method according to claim 41, wherein the addresses are Internet Protocol (IP) addresses.
Claim 43	
43	The method according to claim 32, wherein the packet is an Transmission Control Protocol (TCP) packet that comprises source and destination TCP ports, a TCP sequence number, and a TCP sequence mask fields, and wherein the packet-applicable criterion is that the source TCP port, the destination TCP port, the TCP sequence number, the TCP sequence mask, or any combination thereof, matches a predetermined value or values.
Claim 44	
44	The method according to claim 32, wherein the packet network comprises a Wide Area Network (WAN), Local Area Network (LAN), the Internet, Metropolitan Area Network (MAN), Internet Service Provider (ISP) backbone, datacenter network, or inter-datacenter network.
Claim 45	
45	The method according to claim 32, wherein the first entity is a server device and the second entity is a client device, or wherein the first entity is a client device and the second entity is a server device.

Claim 46	
46	The method according to claim 45, wherein the server device comprises a web server, and wherein the client device comprises a smartphone, a tablet computer, a personal computer, a laptop computer, or a wearable computing device.
Claim 47	
47	The method according to claim 45, wherein the communication with the controller is based on, or uses, a standard protocol.
Claim 48	
48	The method according to claim 47, wherein the standard protocol is according to, based on, or compatible with, an OpenFlow protocol version 1.3.3 or 1.4.0.
Claim 49	
49	The method according to claim 48, wherein the instruction comprises a Type-Length-Value (TLV) structure.
Claim 50	
50	The method according to claim 32, wherein the network node comprises a router, a switch, or a bridge.
Claim 51	
51	The method according to claim 32, wherein the packet network is an Internet Protocol (IP) network, and the packet is an IP packet.
Claim 52	
52	The method according to claim 51, wherein the packet network is a Transmission Control Protocol (TCP) network, and the packet is an TCP packet.
Claim 53	
53	The method according to claim 32, further comprising: receiving, from the first entity over the packet network, one or more additional packets;

	checking, if any one of the one or more additional packets satisfies the criterion; responsive to an additional packet not satisfying the criterion, sending over the packet network, the additional packet to the second entity; and responsive to the additional packet satisfying the criterion, sending the additional packet over the packet network, in response to the instruction.
Claim 54	
54	The method according to claim 32, wherein the packet network is a Software Defined Network (SDN), the packet is routed as part of a data plane and the communication with the controller serves as a control plane.

F. Claim Construction

56. It is my understanding that in order to properly evaluate the '111 Patent, the terms of the claims must first be interpreted. It is my understanding that the claims are to be construed according to the same claim construction standard that district courts use. I have been informed by counsel for Petitioner that the challenged claims of the '111 Patent are to be given their ordinary and customary meaning as understood by one of ordinary skill in the art at the time of the invention in light of the specification and the prosecution history pertaining to the patent.

57. I have reviewed the entirety of the '111 Patent along with the prosecution history of the '111 Patent. In the sections that follow, I provide references from the specification of the '111 Patent for certain terms.

1. The “Controller” Term

58. Independent claims 1 and 32 include the term “controller.” It is my understanding that in other IPR proceedings involving the ’111 Patent, it has been proposed that the term “controller” be construed to mean “an entity configured to perform deep packet inspection on packets.”²

59. I also understand that in a prior district court case involving the ’111 Patent, but that did not involve Petitioner, the district court preliminarily construed the “controller” term to mean “an entity that is capable of controlling deep packet inspection.”

60. In my opinion, the “controller” term does not require construction because the prior art I discuss herein teaches the claimed “controller” under any reasonable construction, including those discussed above, as explained further herein.

² I understand that this construction was previously offered by Cisco Systems, Inc., an unrelated petitioner, in IPR2023-00554. I also understand that Juniper Networks, Inc. filed a petition and a motion for joinder in IPR2024-00037 that was granted by the Board. I also understand that Juniper Networks advocated for this construction in IPR2024-00895 concerning the ’111 Patent.

2. The “Criterion” Terms

61. Claim 1 of the '111 Packet and its dependent claims recite “a packet-applicable criterion” and refer to “the criterion” or “the packet-applicable criterion.” Similarly, Claim 32 recites “the criterion” and its dependent claims refer to “the criterion” or “the packet-applicable criterion.” The terms “packet-applicable criterion” and “criterion” do not appear in the '111 Patent’s specification. But the '111 Patent discloses how “each network node 112 is configured to determine if an incoming packet requires inspection or not,” and that the “determination is performed based on a set of instructions provided by the controller 111.” '111 Patent at 4:12-15. As a result of this set of instructions, the packet “is either redirected to the controller 111 or mirrored and a copy thereof is sent to the controller 111” without alteration. '111 Patent at 4:15-19, 4:61-5:16 (describing type-length-value structures for parsing and identifying packet fields). Further, the '111 Patent includes a series of examples of probe instructions that consider various TCP flags such as the SYNC, ACK, FIN, and RST flags. '111 Patent at 4:26-41. The '111 Patent then states that “each node 112 is configured to receive an incoming packet (either a request from a client device 130 or response from a server 140), analyze the packet’s header, and perform the action (redirect the packet to controller 111 or send to destination server 140) respective of the value of the TCP flag.” '111 Patent at 4:39-46. Given this description, it is my opinion that a POSITA would have

understood the “packet-applicable criterion” and “criterion” to include “the conditions, or basis, used to identify packets for actions, such as inspection.”

VI. TECHNOLOGY BACKGROUND AND STATE OF THE ART

62. Before providing my analysis of the ’111 Patent and the prior art references, as included below, a background discussion of the state of the art of deep packet inspection in software defined networks and the technologies they employ is helpful.

A. Deep Packet Inspection

63. As network utilization continues to grow, bandwidth misuse and security concerns are becoming increasingly prevalent and problematic. *See, e.g.*, EX1008 (M. Liao, et al., “Design and Evaluation of Deep Packet Inspection System: A Case Study,” IET Networks, pp. 1-8 (2012) (“Liao”)). To help mitigate this misuse, network administrators try to identify the network applications operating on the network. In computer networks, an endpoint’s application is identified by a port number. One technique for identifying network applications utilizes this port number information. The Internet Assigned Numbers Authority (IANA) maintains a commonly used listing of well-known port numbers. *See, e.g.*, <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>. Utilizing this or similar listings, network administrators could classify traffic based on the port numbers.

64. But this technique presumes network applications respect this listing instead of using random network ports. See Liao at 1; see also EX1009 (A. W. Moore and K. Papagiannaki, “Toward the Accurate Identification of Network Applications,” In: PAM, Springer, vol. 5, pp. 41-54 (2005) (“Moore”)). And this deficiency was well-known. See Moore at 2, 10-11 (“[M]alware or attack traffic may use the well-known ports of a particular service, thus inflating the amount of traffic attributed to that application.”). Indeed, even in 2005, certain types of traffic sought to mask themselves by using port 80 which HTTP would typically utilize. Moore at 2. And as network administrators increasingly utilized port numbers to classify network traffic, newer network applications avoided the use of well-known ports entirely and instead used different, randomly assigned ports. Moore at 2. To avoid misclassification, network administrators began implementing content-based classification schemes with different levels of complexity. Moore at 4-8.

65. Deep packet inspection (DPI) is one such content-based technique that inspects both the header and the payload of a packet to classify network traffic. ’111 Patent at 1:21-29 (describing DPI as one type of dedicated service); Liao at 1. DPI relies on patterns or signatures contained in payloads for network applications. For example, HTTP relies on GET or PUT methods sent from the client to the server. DPI systems may therefore rely on this signature to classify this traffic. Liao at 1.

Some early DPI systems applied regular expressions and string-matching algorithms like Wu-Manber to classify traffic. Liao at 2.

66. Another early DPI system utilized the Netfilter framework contained in the Linux kernel's IP layer. *See generally* Liao. First, the implementers used a core switch's port mirroring function to clone all the packets in the LAN for inspection. Liao at 2.

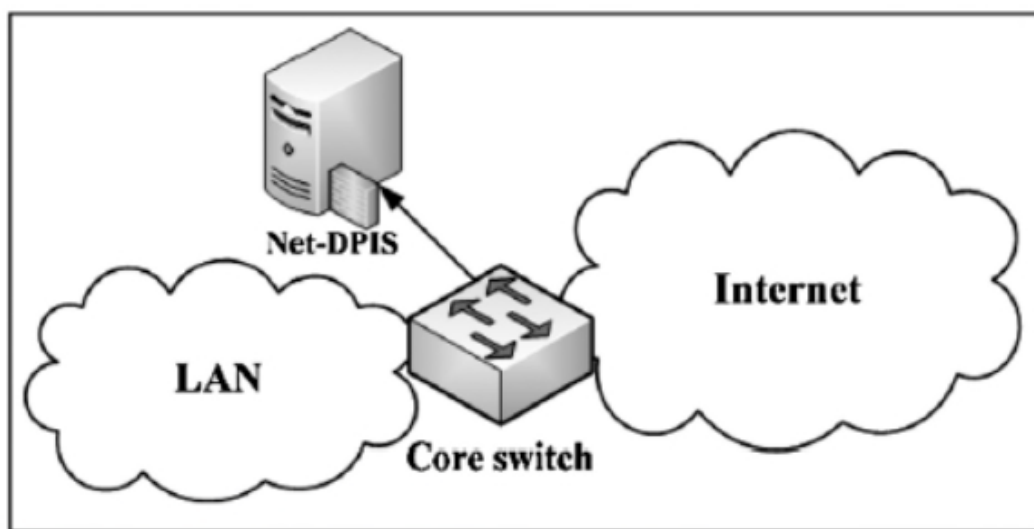


Fig. 3 *Network topology (port mirror)*

67. Then, using the Netfilter framework included as part of the Linux kernel's IP layer, the implementers created a system with a set of four types of matching policies to search for signatures in the packet. Liao at 3-4. With an identified signature, the rule table identifies the service type. Liao at 3-4. The implementers here utilized a personal computer to perform their experiments and

found their technique improved on the performance over those using other DPI techniques. Liao at 5, 7.

B. Software-Defined Networking

68. In networking, the concept of a control plane and a data, or forwarding, plane define where certain processes necessary for networking occur. The control plane determines how the forwarding plane should handle forwarding packets from one place to another. EX1010, RFC 3654 at 4-5 (available at <https://www.rfc-editor.org/rfc/rfc3654>) (“RFC 3654”). Data, or forwarding, planes process the packets arriving on inbound interfaces in accordance with the control plane’s decisions. RFC 3654 at 4-5. The control plane implements management protocols and dictates the forwarding behavior of the data plane by, for example, manipulating the forwarding tables, the state of the interfaces, or by adding or removing Network Address Translation (NAT) bindings. RFC 3654 at 4-5. The data plane handles per-packet processing and performs functions including layer 3 forwarding, metering, shaping, firewalling, NAT, encapsulation, decapsulation, and encryption. RFC 3654 at 4-5. Traditionally, both the control and data planes existed in the same hardware device. For example, the Cisco ASR 1000 series routers and Nexus 7000 series switches separated the control and data planes so that active and standby control planes existed to facilitate fault tolerance and transparent software upgrades. *See*,

e.g., EX1011 (W. Xia, et al., “A Survey on Software-Defined Networking,” IEEE Communication Surveys & Tutorials, Vol. 17, No. 1, pp. 27-51 (June 13, 2014)).

69. But as early as April 2004, there existed a desire to separate these different planes into different physical components for certain applications. The Forwarding and Control Element Separation (ForCES) framework sought to define protocols for standardized communication between control and forwarding planes so that the planes could “become physically separated standard components.” EX1012, 5-6 (“RFC 3746”) (available at <https://www.rfc-editor.org/in-notes/rfc3746.txt>). The authors of ForCES believed this standardization would increase design choices and flexibility, while facilitating more rapid innovation for the control and data plane components. RFC 3746 at 5-6.

70. In April 2008, a whitepaper describing OpenFlow was published. See EX1013 (N. McKeown, et al., “OpenFlow: Enabling Innovation in Campus Networks,” ACM SIGCOMM Computer Communication Review, vol. 38, No. 2, pp. 69-74 (April 2008) (“McKeown”)). The authors recognized a need for programmable networks that would facilitate testing of new network architectures and distributed systems. McKeown at 1. The authors created OpenFlow to facilitate programming of the flow tables in these devices using common sets of functions shared by many switches and routers. McKeown at 2. OpenFlow defined a basic set of actions for all OpenFlow devices. McKeown at 2. OpenFlow controllers

remotely control the packet forwarding tables of OpenFlow compliant devices using this defined set of actions. McKeown at 3-4; *see also* EX1005, 4:30-40 (describing OpenFlow SDNs); EX1006, 1:25-41 (same).

71. Using OpenFlow, implementers, including some of the world's largest companies, have created SDNs to support their operations. For example, in 2012, Google publicly disclosed that it used OpenFlow to control its software-defined network (SDN). *See* EX1014 (S. Levy, "Going with the Flow: Google's Secret Switch to the Next Wave of Networking," (available at <https://www.wired.com/2012/04/going-with-the-flow-google/>)).

72. As discussed above, prior to the assumed April 22, 2014 priority date of the '111 Patent, all of the technology at issue in the challenged claims was well known and broadly applied in various commercial applications. In my opinion, no individual elements of the challenged claims of the '111 Patent were novel at the time of the alleged invention, and there was nothing novel or inventive about the manner in which those elements were combined in the challenged claims. Further, there were no technological barriers to combining these known elements to form the claimed inventions. Indeed, combining these elements would have yielded predictable results.

VII. APPLICATION OF THE PRIOR ART TO THE CHALLENGED CLAIMS

73. I have been asked to provide my opinion as to whether the challenged claims of the '111 Patent would have been obvious in view of the prior art. The discussion below provides a detailed analysis of how the prior art references I reviewed disclose, teach, or suggest the limitations of the challenged claims of the '111 Patent.

74. As part of my analysis, I have considered the scope and content of the prior art and any potential differences between the claimed subject matter and the prior art. I have conducted my analysis as of the assumed priority date of the '111 Patent: April 22, 2014. I have also considered the level of ordinary skill in the pertinent art as of that date.

75. Below, I describe in detail the scope and content of the prior art, as well as any differences between the subject matter claimed and the prior art, on an element-by-element basis for each challenged claim of the '111 Patent. The analysis supports my finding that the differences between the claims of the '111 Patent and the prior art discussed herein are such that the subject matter as a whole would have been obvious at the time of the priority date of the '111 Patent to a POSITA.

76. In the grounds below, I describe on an element-by-element basis how the prior art discloses or teaches all elements of Claims 1-54 of the '111 Patent.

A. Grounds of Unpatentability

77. I have reviewed and analyzed the prior art references and materials listed in Section III above. In my opinion, the challenged claims of the '111 Patent are rendered obvious based on the following prior art set forth in Grounds 1-3 below:

Ground	'111 Patent Claims	Basis for Challenge under §103
1	1-6, 9-15, 18-19, 21-36, 41-42, 44-54	Lefebvre in view of Chua
2	7-8, 37-38	Lefebvre and Chua in further view of Rash
3	16-20, 39-43	Lefebvre and Chua in further view of RFC 793

B. Summary of Prior Art

1. Overview of Lefebvre (Exhibit 1005)

78. U.S. Patent No. 10,097,452 (“Lefebvre”) is titled “Chaining of Inline Services Using Software Defined Networking.” Lefebvre at Cover (INID code (54)). It is my understanding that the U.S. Patent and Trademark Office (“Patent Office”) didn’t consider Lefebvre during the prosecution of the '111 Patent.

79. Lefebvre was filed on July 24, 2012, published on October 17, 2013, and issued on October 9, 2018. Lefebvre at Cover (INID code (22), (65), (45)). I understand that Lefebvre qualifies as prior art under 35 U.S.C. § 102(a)(1)-(2).

80. Lefebvre discloses that network operators deploy various middleboxes or inline services to “inspect and alter network traffic transiting through their

network.” Lefebvre at 1:19-27. End users do not notice this inspection and alteration of network traffic, which includes “transparent caching, virus scanning, and deep packet inspection.” Lefebvre at 1:21-25. These services typically exist as dedicated appliances that come with their own costs. Lefebvre at 1:25-27. As network traffic demands increase, network operators desire the ability to selectively direct traffic to these middleboxes or inline services to minimize these costs. Lefebvre at 1:28-32. Lefebvre discloses an example where the network operator directs video traffic away from DPI to minimize costs. Lefebvre at 1:34-38. Lefebvre also discloses that network operators may obtain new revenue sources as users purchase services executed by these middleboxes or inline services. Lefebvre at 1:39-43.

81. Lefebvre discloses that traffic steering is “the action of classifying traffic and directing the different classes of traffic through specific service chains.” Lefebvre at 1:44-47. Service chains are ordered sets of services. Lefebvre at 1:44. Although there exist solutions for implementing traffic steering, each have their own drawbacks. For example, third-party service applications cannot integrate with an extensible router or gateway through additional service cards due to the proprietary nature of these service cards. Lefebvre at 1:65-2:5. The scalability of this approach is also limited by the router or gateway’s capacity. Lefebvre at 2:3-5. As another example, routers using policy based routing (PBR) to classify and forward traffic to

static service chains do not support defining network policies in a centralized manner and requires each service to configure and classify traffic to the next appropriate service. Lefebvre at 2:6-11. Static service chains also do not accommodate subscribers each having different sets of subscribed services. Lefebvre at 2:11-17. And as a final example, services configured to return traffic to routers using PBR after processing forces the router to classify and redirect large amounts of traffic. Lefebvre at 2:18-21.

82. Instead, Lefebvre discloses how network operators define service policies specifying traffic classes and the service chains each traffic class traverses. Lefebvre at 4:41-47. Lefebvre discloses implementing an SDN using a standardized protocol like OpenFlow which includes support for multiple tables and a metadata field for exchanging information between tables. Lefebvre at 4:30-40. Lefebvre discloses these features help “reduce the number of rules by avoiding cross-products that occur when flattening multi-step classifications.” Lefebvre at 4:37-40.

83. Lefebvre implements traffic steering using a two-step process. First, it classifies incoming packets and assigns a service path based on predefined policies. Lefebvre at 6:17-19, Abstract. Then the packets are forwarded to the next service based on the packet’s position in the assigned service path. Lefebvre at 6:20-21. For example, if the assigned service chain includes four different services A, B, C, D, the packet is forwarded to service A, then service B, then service C, and finally

service D. Lefebvre's traffic steering process supports three types of policies: subscriber-based, application-based, and flow-based. Lefebvre at 6:26-28. Lefebvre's subscriber-based policies specify the subscriber's IP address and the set of services each subscriber's traffic should traverse. Lefebvre at 6:32-35. Application-based policies specify either an IP address block and/or a UDP/TCP port on a per application basis, and apply those policies to all subscribers. Lefebvre at 6:38-41. These refine subscriber-based policies by adding or removing services from the set of services specified in the subscriber-based policies. Lefebvre at 6:41-45. And flow-based policies are specific to a single flow or IP 5-tuple (i.e., source IP address, destination IP address, protocol, source port, destination port). Lefebvre at 6:46-48. These dynamically override subscriber-based and application-based policies for specific flows and redirect flows, even mid-flow, to different sets of services. Lefebvre at 6:48-53.

84. Once an operator defines service policies with traffic classes and service chains, Lefebvre discloses that a centralized controller translates these policies into rules for the programmable switches that steer the network traffic through the service chains. Lefebvre at 4:43-47. Service instances can exist in multiple service chains and operators can locate and chain these service instances arbitrarily. Lefebvre at 4:48-53. And steering traffic at finer granularity including subscribers and traffic types is supported. Lefebvre at 4:53-54.

2. Overview of Chua (Exhibit 1006)

85. U.S. Patent No. 9,264,301 (“Chua”) is titled “High Availability for Software Defined Networks.” Chua at Cover (INID code (54)). It is my understanding that the Patent Office did not consider Chua during the prosecution of the ’111 Patent.

86. Chua was filed on March 15, 2013 and issued on February 16, 2016. Chua at Cover (INID code (22), (45)). I understand that Chua qualifies as prior art under 35 U.S.C. § 102(a)(2).

87. Chua discloses that SDNs generally use a standalone controller that “determines the routes and program other devices in the network to behave according to the determinations made by the controller.” Chua at 1:25-35; *see also* Chua at 1:45-55 (describing the control plane being “physically separate from the data plane (or forwarding plane) for an SDN”). Physical or virtual instances form the components of the SDN. Chua at 1:52-54. Protocols including OpenFlow facilitate this ability. Chua at 1:35-41, 23:62-24:4 (describing OpenFlow as “an example of an SDN protocol”).

88. Chua discloses that the SDN controller controls the various devices including network devices and service devices. Chua at 6:25-28. Using data from the service devices, Chua’s SDN controller may make network enforcement decisions including allowing, blocking, mirroring, redirecting, transforming, and

encapsulating the packets of the packet flow. Chua at 7:33-54. Chua also discloses that in these networks, service devices may exist to provide additional functionality, including intrusion detection, intrusion prevention, web proxies, web servers, denial of service (DoS) protection, traffic filtering, malware detection, anti-virus, packet capture and analysis, and honeypots. Chua at 5:50-6:24.

89. In addition to controlling the SDN, Chua discloses the controller may execute other programs. Chua at 6:36-52. Chua discloses that the controller may host additional services, including Layer 4-Layer 7 services, instead of (or in addition to) external service devices. Chua at 6:42-45. Chua also discloses that Layer 3 applications could execute in the SDN. Chua at 6:45-52. Chua discloses that in such a configuration, the controller may augment these other programs, which are executing on the controller, by continuing to perform its SDN functions as well. Chua at 6:45-52 (describing a Layer 3 routing stack executing on the controller, and the controller commanding network devices to update forwarding tables in response). In particular, Chua discloses the controller may perform DPI on packets from client devices. Chua at 10:48-52, 31:48-59.

3. Overview of Rash (Exhibit 1007)

90. U.S. Patent No. 9,813,447 (“Rash”) is titled “Device and Related Method for Establishing Network Policy Based on Applications.” Rash at Cover

(INID code (54)). It is my understand that the Patent Office did not consider Rash during the prosecution of the '111 Patent.

91. Rash was filed on March 15, 2013, published on September 18, 2014, and issued on November 7, 2017. Rash at Cover (INID code (22), (65), (45)). I understand that Rash qualifies as prior art under 35 U.S.C. § 102(a)(2).

92. Rash discloses a network that adjusts policies associated with the operation of devices on the network. Rash at Abstract. Rash discloses “snooping” of the network traffic flows to identify applications operating on the network. *See, e.g.*, Rash at 6:22-40. Rash discloses using signatures, heuristics, and other techniques including “port values, protocol values, statistics analysis, customized programs dependent on characteristics unique to a program and OSI layer 2 information.” Rash at 6:50-57. To process this information, Rash discloses a targeted approach where packets, or portions of packets, are mirrored to a destination other than the original intended destination. *See, e.g.*, Rash at 7:51-59, 9:3-12, 25:30-55, 26:11-35, 27:31-43, 29:58-62, 35:66-36:2. Rash discloses that a network control manager controls the mirroring function. Rash at 9:12-15, 29:46-30:17. Rash discloses the applicability of its dynamic traffic mirroring function for intrusion detection systems and network access control, among other applications. Rash at 10:29-56. And Rash discloses this dynamic mirroring functionality helps minimize the data mirrored to identification appliances or other infrastructure

devices configured to carry out the application identification function. Rash at 12:59-13:8, 34:43-51.

4. Overview of RFC 793 (Exhibit 1015)

93. RFC 793 is titled Transmission Control Protocol, Darpa Internet Program Protocol Specification and was published in September 1981, more than 30 years before the assumed priority date of the '111 Patent. RFC 793 at 1. RFC 793 defines the well-known Transmission Control Protocol and would have been widely known to POSITAs at the time the '111 Patent was filed.

94. “Request for Comments” (RFC) documents published by the Internet Engineering Task Force (IETF) were well-known as of the priority date of the '111 Patent, and it is my opinion that they were “printed publications” for the purposes for which they are cited throughout. As further evidence of its public availability before the assumed priority date of the '111 Patent, RFC 793 was cited in U.S. Patent Application Publication No. 2007/0094411. *See* EX1026, ¶0063. A POSITA in the field of network communications, including software defined networks, would have reasonably relied upon such documents.

C. Ground 1: Claims 1-6, 9-15, 18-19, 21-36, 41-42, and 44-54 are rendered obvious by Lefebvre in view of Chua

95. As I discussed above in Section VI, well before 2014, both SDN and DPI were well-known and ubiquitous. For example, both Lefebvre and Chua discuss SDN and DPI. Lefebvre at 1:21-25, 1:34-38; Chua at 10:48-52, 31:48-59. Lefebvre

and Chua both disclose how DPI often executes in dedicated service devices. Lefebvre at 1:21-25, 1:34-38; Chua at 31:54-59 (describing DPI service devices). And Chua specifically discloses the SDN controller performing DPI as well. Chua at 31:48-54.

96. Based on the following analysis, I conclude that a POSITA at the relevant time (April 22, 2014) would have understood the limitations of Claims 1-6, 9-15, 18-19, 21-36, 41-42, and 44-54 were expressly disclosed, taught, or suggested by Lefebvre in combination with Chua. In my opinion, a POSITA would have found Claims 1-6, 9-15, 18-19, 21-36, 41-42, and 44-54 obvious in view of Lefebvre and Chua.

1. Motivation to Combine Lefebvre and Chua

97. It is my opinion that a POSITA would have been motivated and found it obvious to modify Lefebvre with Chua's teachings. Lefebvre discloses techniques for an SDN to steer traffic through inline services. Lefebvre at 1:13-21, 2:39-47. Lefebvre discloses how operators can define the traffic classes and service chains for those classes for processing traffic flows on a per packet basis. Lefebvre at 4:41-43. Lefebvre discloses these operator instructions are programmed into the switches as rules so that the network traffic passes through the ordered chain of services as desired. Lefebvre at 4:41-47. Lefebvre discloses that at least some of the switches in the SDN use OpenFlow. See Lefebvre at 5:41-44. Once defined by the operator

and programmed into the switches, Lefebvre discloses that traffic steering requires classification of incoming packets and assignment of a service path based on predefined policies. Lefebvre at 6:17-19. Then the packets are forwarded to the next service in the assigned service path. Lefebvre at 6:20-21.

98. Lefebvre identifies several types of services that could form part of the service chain, including DPI. Lefebvre at 1:28-38, 4:48-54. Regarding DPI, Lefebvre discloses “[t]hese services are usually packaged and sold as dedicated appliance (either physical or virtual) and are often expensive.” Lefebvre at 1:25-27, 1:34-38. One reason Lefebvre offers for implementing traffic steering is to direct traffic that does not require inspection away from expensive services like DPI, reducing the need to invest in new service appliances. Lefebvre at 1:32-38. Lefebvre discloses that service nodes, separate from the controller, form the service chain. See Lefebvre at 6:28-31, FIG. 1. Lefebvre therefore controls the usage of DPI services by routing network traffic through the service only as appropriate, where the services are separate from the controller.

99. Like Lefebvre, Chua discloses using an SDN where a controller determines the behavior of devices in the network and how traffic flows through the network. Chua at 1:25-35. Like Lefebvre, Chua also discusses OpenFlow. Specifically, Chua discloses protocols including OpenFlow that controls the data-plane devices of the network. Chua at 1:35-41. These network devices provide data

to Chua's controller, which then makes network enforcement decisions. Chua at 6:25-28. Chua's controller considers the traffic on a per-packet or per-flow basis as necessary. Chua at 7:33-54, 10:48-52, 15:9-17. Chua's controller then programs network devices of the SDN to implement these decisions. Chua at 7:33-54 (describing different programmed actions taken "on packets of a packet flow"), 31:30-34. Chua's service devices include those that execute DPI, for example, along with other techniques including intrusion detection service and firewalls (e.g., web-application firewalls). Chua at 5:59-67, 10:48-52, 15:4-9, 16:30-33, 31:48-50, Fig. 9 (step 402). Chua also discloses that the SDN controller may execute other programs, including Layer 4-Layer 7 services, instead of external service devices. Chua at 6:36-52, 6:42-45 ("For example, SDN controller 112 itself may host one or more L4-L7 services, **rather than** (or in addition to) services, provided by service devices 116.") (emphasis added). And Chua discloses the controller performing DPI. Chua at 10:48-52, 15:4-9, 16:30-33, 31:48-50.

100. A POSITA would have been motivated and found it obvious to modify Lefebvre with Chua's teachings because both describe SDNs, and both describe DPI as one type of service in an SDN. Lefebvre at 1:28-38; Chua at 10:48-52, 15:4-9, 16:30-33, 31:48-50, Fig. 9 (step 402). And both Lefebvre and Chua disclose use of OpenFlow devices. Lefebvre at 5:41-44; Chua, 1:35-41. Lefebvre and Chua are

therefore in the same field of endeavor and contain overlapping disclosures with similar purposes.

101. Modifying Lefebvre in view of Chua's teachings would have been obvious to a POSITA. Lefebvre has three different levels of policies which have different levels of granularity. Lefebvre's subscriber-based policies rely on the subscriber's IP address. Lefebvre at 6:32-35. Lefebvre's application-based policies rely on an IP address block and/or a UDP/TCP port on a per application basis, and apply to all subscribers. Lefebvre at 6:38-41. These application-based policies refine subscriber-based policies by adding/removing services from the services specified in subscriber-based policies. Lefebvre at 6:42-45. Both Lefebvre's subscriber-based and application-based policies operate on the packets being received by the SDN. And Lefebvre's flow-based policies specify the flow or IP 5-tuple (i.e., source IP address, designation IP address, protocol, source port, and destination port). Lefebvre at 6:46-48. Similarly, Chua discloses that the SDN determines "the appropriate type of flow troubleshooting that includes the appropriate IP ranges to watch on, and the TCP/UDP services that the flowchain is meant to service." Chua at 18:9-16. And Chua discloses that the SDN controller performs DPI "on packets from client device[s]." Chua at 31:48-50; *see also* Chua at 7:33-54 (describing enforcement actions "on packets of a packet flow"), Fig. 9

(step 402). Lefebvre and Chua therefore share similar techniques for classifying the traffic traversing their networks.

102. A POSITA would have been motivated to look to Chua's more detailed teachings regarding actions an SDN controller takes in response to information from security-related services like DPI and apply them to Lefebvre. Lefebvre mentions DPI as one type of known service, but focuses its disclosure on actions relevant to traffic steering and the passing of the packet through assigned service chains including redirecting or dropping the packet. See Lefebvre at 6:17-31, 1:28-38 (discussing DPI); see also Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions). Lefebvre does not expressly disclose specifics regarding actions resulting from the services processing the traffic along the service path. See generally Lefebvre. For example, when implementing DPI in an SDN like Lefebvre's, a POSITA would have needed additional disclosures regarding actions taken after DPI identifies malicious traffic. Chua discloses these details regarding actions an SDN controller may take in response to the information provided by security-related services like DPI, including allowing, blocking, mirroring, redirecting, transforming, or encapsulating the network traffic. Chua at 7:33-54. A POSITA would therefore have looked to Chua's more detailed teachings regarding actions an SDN controller takes in response to information from services like DPI and apply them to Lefebvre when implementing DPI in the SDN.

103. Chua also discloses that the controller may execute other programs instead of external service devices. Chua at 6:42-45. A POSITA would have been motivated to modify Lefebvre with this teaching from Chua for multiple reasons. Lefebvre discloses that services including DPI “are usually packaged and sold as dedicated appliances (either physical or virtual) and are often expensive.” Lefebvre at 1:25-27, 1:34-38. Chua, however, discloses programming an SDN controller to perform DPI and other functions that may be performed by a service device. Chua at 31:48-50, 6:42-45. A POSITA would recognize Chua’s teaching to mean that performing DPI and other services is not an expensive task that only dedicated appliances can execute, but a task that an SDN controller could execute. Incorporating DPI in Lefebvre’s controller, as Chua teaches, would remove the need for the expensive dedicated appliance that Lefebvre discloses existed in the prior art.

104. A POSITA would have also been motivated to modify Lefebvre with Chua’s programmable controller teachings because Chua discloses how programs executing on the controller may utilize the SDN controller’s existing abilities to implement appropriate updates to the SDN to facilitate the programs’ functionality. Chua at 6:36-52. For example, “[u]sers of SDN controller 112 may be provided with the ability to create programs that are executable by SDN controller 112.” Chua at 6:36-39. That is, in addition to directing the upstream traffic to different application server(s), “SDN controller 112 itself may host one or more L4-L7 services, rather

than (or in addition to) services provided by service devices 116.” Chua at 6:42-45. A POSITA would have known that this programmable feature of SDN controller 112 is highly desirable for use in Lefebvre to reduce “the high cost of service appliances.” Lefebvre at 1:30-32. And including within the controller the service device’s functionality, as Chua teaches, would remove the need to address network failures between endpoints that Chua states is a “complex problem,” and that would also apply to network failures between network devices, the SDN controller, and the DPI service device. *See* Chua at 19:1-53 (describing redundancy possibilities for SDN appliances). Chua’s controller teachings therefore help simplify the SDN and reduce the need to address certain types of failures in the SDN. A POSITA would therefore have motivation to consider Chua’s teachings.

105. Implementing Chua’s teachings in Lefebvre’s controller would have been well within the skill of a POSITA, and the POSITA would have had a reasonable expectation of success. Lefebvre already discloses redirecting packets to the appropriate service. Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions). Chua discloses additional actions an SDN controller may take in response to the information provided by services such as DPI like allowing, blocking, mirroring, redirecting, transforming, or encapsulating the network traffic. Chua at 7:28-54. Implementing these additional actions would have been straightforward and simple for a POSITA because these additional actions taught by

Chua would simply build on standard actions many networking devices already implement, and Lefebvre already discloses redirecting of packets. See Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions). For example, in the paper proposing OpenFlow, the authors stated that OpenFlow switches support basic actions including forwarding, encapsulating, and dropping packets. McKeown at 3.

106. Implementing a DPI service in Lefebvre's controller, as Chua teaches, would also have been straightforward and simple for a POSITA. Although Lefebvre omits detailed discussion of its controller, it is my opinion that a POSITA would recognize that Lefebvre's controller includes components including processors and memory. Chua confirms how controllers include a control unit with "one or more processors and/or computer readable memory for storing software or firmware instructions." Chua at 10:67-11:6, 31:60-32:6. And Lefebvre discloses that embodiments of what it describes may exist as a software product executing programs. Lefebvre at 17:17-37. Similarly, Chua discloses its controller is programmable when describing how "a software development kit (SDK) may be provided for creating programs that can be executed" by the SDN controller. Chua at 6:38-40. An SDK helps a programmer create applications by providing application programming interfaces (APIs) tailored for a specific hardware platform, operating system, or combination of both. SDKs may also include debugging tools

or other tools to help programmers when creating applications. As an example, Chua discloses how an SDN controller performs DPI on packets from a client device. Chua at 31:49-54. It is therefore my opinion that nothing more than the routine skill of a POSITA would be required to implement Chua's teachings in Lefebvre.

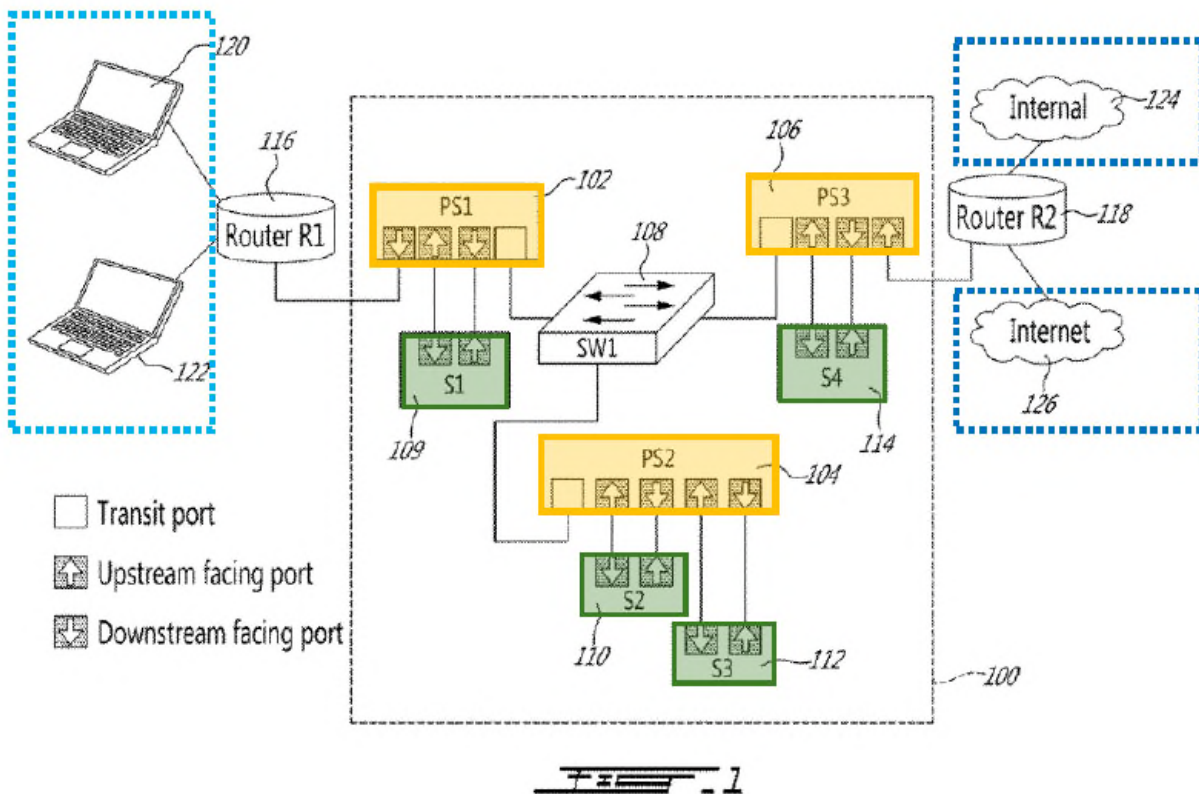
107. And a POSITA would have had a reasonable expectation of success in modifying Lefebvre with Chua's controller teachings. Lefebvre discloses that embodiments of what it describes may exist as a software product executing programs. Lefebvre at 17:17-37. This confirms my prior opinion that a POSITA would recognize that Lefebvre's controller includes components including processors and memory. Chua discloses how, by using the SDK, users may create "one or more L4-L7 services," or an L3 application, that execute on the controller "rather than" on service devices. Chua at 6:37-47. Chua also discloses how the programs may use features of the SDN controller, including commanding network equipment to update forwarding tables. Chua at 6:47-52. And as an example, Chua discloses how an SDN controller performs DPI on packets from a client device. Chua at 31:49-54. Because Lefebvre discloses how its embodiments exist as software programs, and Chua discloses the inclusion of an SDK and example programs executing on its controller including DPI, it is my opinion that a POSITA would have had a reasonable expectation of success in implementing services (e.g., a DPI service) in Lefebvre's controller, as Chua teaches.

2. Claim 1

- (i) **1[Pre]: A method for use with a packet network including a network node for transporting packets between first and second entities under control of a controller that is external to the network node, the method comprising:**

108. If the preamble is limiting, the combination of Lefebvre and Chua renders it obvious.

109. Lefebvre discloses how operators “define service policies that specify traffic classes and the chain of services that each class must traverse” and how the “policies are translated by the controller into rules that are programmed on the switches in the service network.” Lefebvre at 4:41-47; *see also* Lefebvre at 1:13-21. Lefebvre discloses that the traffic steering process supports three types of service policies: subscriber-based policies, application-based policies, and flow-based policies. Lefebvre at 6:26-28. Below, I reproduce annotated FIG. 1 of Lefebvre from Dr. Mir’s declaration in IPR2024-00895 to highlight certain components.



Lefebvre at FIG. 1 (annotated).

110. Lefebvre discloses that incoming traffic “always enters the service network 100 via a perimeter switch and through a node port,” and that arriving packets are processed and steered to the next node in the assigned service paths. Lefebvre at 6:5-11. Lefebvre discloses **user equipment 120, 122** connected to router R1 and the **internal network 124** and the **Internet 126** connected to router R2. Lefebvre at 5:38-54, 6:13-16. Lefebvre’s user equipment, internal network, and Internet therefore disclose the “packet network” and “first and second entities.”

111. Lefebvre’s service network includes **perimeter switches 102, 104, 106** and an inner switch SW1. Lefebvre at 5:38-44. The network also includes **services**

109, 110, 112, 114. EX1005, 5:44-47. Lefebvre discloses that the **perimeter switches 102, 104, 106** may be OpenFlow switches whereas the inner switch 108 may be “either an OpenFlow switch or a plain Ethernet switch.” Lefebvre at 5:41-44. Each of Lefebvre’s **perimeter switches 102, 104, 106** therefore disclose the “network node” of the claims because they, like the ’111 Patent’s network nodes, communicate with the central controller using OpenFlow. See ’111 Patent at 3:47-48.

112. And even though Lefebvre states that the centralized controller is “not shown in FIG. 1,” Lefebvre discloses a centralized controller pushes these policies to the relevant switches. Lefebvre at 6:28-31 (“These policies can be specified by the operator and pushed to the relevant switches by a centralized controller[.]”). A POSITA would therefore understand that Lefebvre’s controller is external to the **perimeter switches 102, 104, 106**, especially given that Lefebvre’s system involves an SDN. See, e.g., Chua at 1:27-29 (“In general, software defined networks involve the use of a standalone controller that performs the control functionality for a set of network devices.”), 1:46-51 (“A software defined network is generally a network of interconnected computing devices having forwarding planes or data planes that can be programmed remotely by one or more controller devices.”). Furthermore, Lefebvre describes using OpenFlow 1.1. Lefebvre, 4:30-40. OpenFlow 1.1 uses “an external controller” as shown in Figure 1 below:

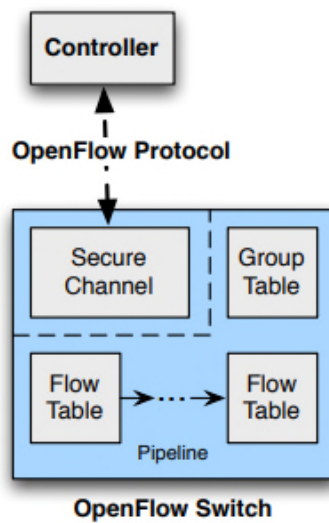


Figure 1: An OpenFlow switch communicates with a controller over a secure connection using the OpenFlow protocol.

EX1027, 3, Fig. 1.

113. And as discussed in Section VII.C.1, a POSITA would have been motivated and found it obvious to apply Chua’s teachings to Lefebvre’s SDN controller. Like Lefebvre, Chua teaches the use of an SDN controller 112 that is external to network devices 108, 110, which Chua teaches may be “switches”:

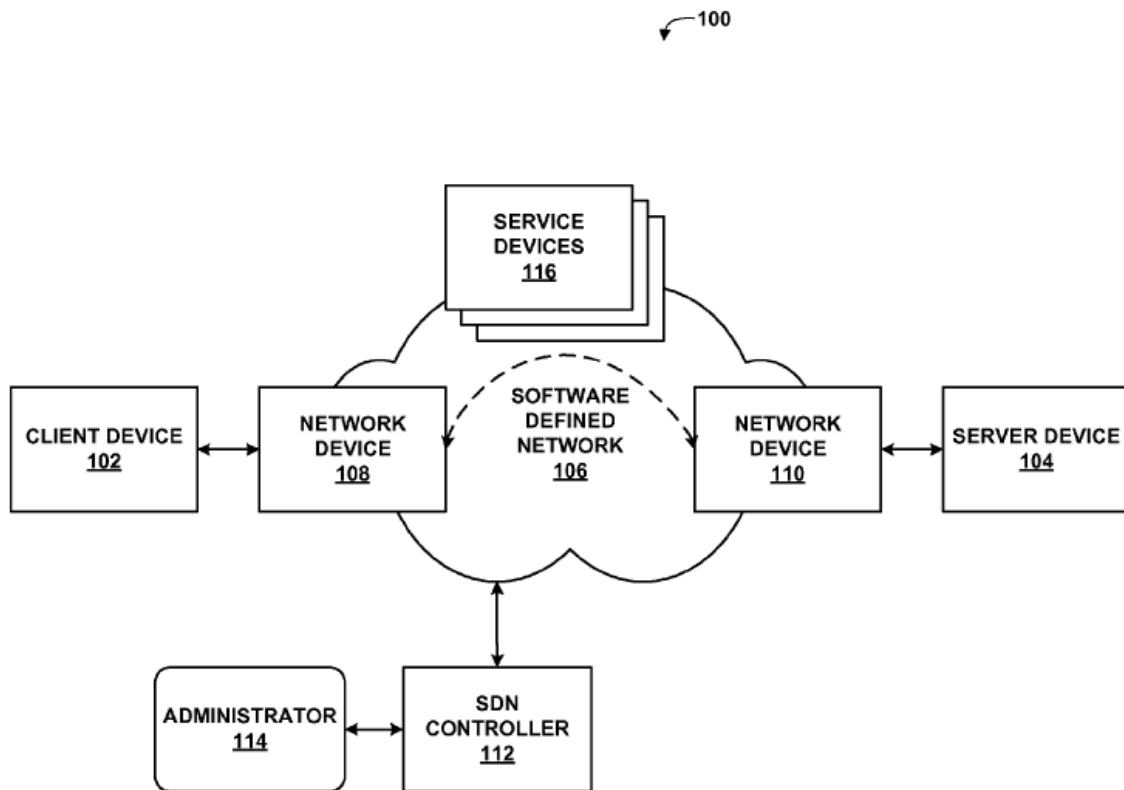


FIG. 1

Chua, FIG. 1, 5:32-37. In the combined system, Lefebvre’s modified controller would then be programmed to execute DPI, as Chua teaches. As I explained in Section VII.C.1, because Lefebvre discloses embodiments that already redirect packets to appropriate services and embodiments existing as software programs, a POSITA would have had a reasonable expectation in success in implementing Chua’s teachings in Lefebvre’s controller. And as a result of this modification, a POSITA would recognize that Lefebvre’s modified controller discloses the claimed “controller,” even if construed to mean “an entity that is capable of controlling deep

packet inspection” or “an entity configured to perform deep packet inspection on packets,” as discussed in Section V.F.1.

114. Thus, the combination of Lefebvre and Chua renders obvious claim element 1[pre].

(ii) 1[a]: sending, by the controller to the network node over the packet network, an instruction and a packet-applicable criterion;

115. The '111 Patent uses the word “instruction” in its specification to describe certain commands including “probe instructions,” “mirroring instructions,” and “termination instructions.” *See, e.g.*, '111 Patent at 4:23-26; *see also* '111 Patent at 4:26-46 (describing redirecting, forwarding, and terminating instructions), 4:47-56 (describing mirroring instructions). As discussed in Section V.F.2, the term “packet-applicable criterion” does not appear in the '111 Patent’s specification. And as discussed in Section V.F.2, it is my opinion that a POSITA would understand a “packet-applicable criterion” to include the conditions, or basis, used to identify packets for actions, such as inspection.

116. Lefebvre discloses that the operator defines “service policies that specify traffic classes and the chain of services that each class must traverse.” Lefebvre at 4:43-45. Lefebvre discloses that the controller programs the rules into the switches of the service network, and the “rules steer the network traffic through the ordered chain of services as specified by the policies.” Lefebvre at 4:43-47,

Table 1, Table 2 (depicting OpenFlow switch table actions), FIG. 5. And Lefebvre discloses that traffic steering is a two-step process. Lefebvre at 6:17-18. The first step “classifies incoming packets and assigns them a service path based on predefined policies.” Lefebvre at 6:18-19, 7:35-8:48 (describing “an example methodology for processing and classifying a packet”), FIG. 2, FIG. 5 (step 510). And the second step “forwards packets to a ‘next’ service based on its current position along its assigned service path.” Lefebvre at 6:20-21, FIG. 5 (step 530).

117. A POSITA would have understood that Lefebvre’s traffic steering involving classification of incoming packets to assign them a service path discloses the claimed packet-applicable criterion. Lefebvre’s traffic steering policies include subscriber-based policies, application-based policies, and flow-based policies. Lefebvre at 6:26-31. Lefebvre’s traffic steering mechanism presumes that all traffic traversing the service network is subscriber traffic. Lefebvre at 5:19-37. But as Lefebvre also discloses, when the traffic is not subscriber traffic, the SDN functions as a simple router that “does conventional destination-IP-based forwarding” where the traffic does not traverse inline services. Lefebvre at 14:23-33. Lefebvre also classifies traffic based on the incoming port, the packet’s destination MAC address, the source or destination IP address, the IP address and/or protocol and/or port number, and the position of the packet on the service path. Lefebvre at 7:35-8:48 (describing “an example methodology for processing and classifying a packet”),

Table 1, Table 2 (depicting OpenFlow switch table actions). These classification techniques disclosed by Lefebvre disclose the claimed packet-applicable criterion because they are the conditions, or basis, used to identify packets for actions. Lefebvre discloses the classification decides which service path the packet will traverse. Lefebvre's next destination table routes the packet to the appropriate service. Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions). Like the '111 Patent's claimed packet-applicable criterion, Lefebvre's classification techniques depend on instructions provided by the controller and determine which service chain the packet will traverse. See '111 Patent at 4:12-46.

118. A POSITA would have also understood that Lefebvre's traffic steering involving classification of incoming packets to assign them a service path discloses the claimed instruction. Lefebvre's final table, the "next destination table," matches the packet to the appropriate service. Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions). Like the '111 Patent's instruction, Lefebvre's final table redirects the packet to the appropriate service. Lefebvre therefore discloses the claimed "an instruction and a packet-applicable criterion."

119. And Lefebvre's controller, as modified by Chua's teachings, similarly discloses "sending, by the controller to the network node over the packet network, an instruction and a packet-applicable criterion." As discussed above, Lefebvre's traffic steering process "supports three types of service policies: subscriber-based

policies, application-based policies, and flow based policies.” Lefebvre at 6:26-28. Lefebvre teaches that “[t]hese policies can be specified by the operator and pushed to the relevant switches by [the] centralized controller[,]” which a POSITA would have understood to teach sending, by the controller to the network node (e.g., one or more of perimeter switches 102, 104, 106), the instruction and the packet-applicable criterion. Lefebvre, 6:28-31. Chua similarly discloses the controller programs network devices “to perform programmed actions on packets” including allowing, blocking, mirroring, redirecting, transforming, and encapsulating packets. Chua at 7:28-54. Lefebvre’s controller already redirects. *See* Lefebvre at 8:49-65, Table 1, Table 2 (depicting Open-Flow switch table actions). As modified by Chua’s teachings, Lefebvre’s controller’s instructions would include the allowing, blocking, and mirroring packets.

120. Thus, the combination of Lefebvre and Chua discloses claim element 1[a].

(iii) 1[b]: receiving, by the network node from the controller, the instruction and the criterion;

121. The combination of Lefebvre and Chua renders obvious claim element 1[b].

122. For the reasons discussed above for element 1[a], a POSITA would have understood that Lefebvre’s traffic steering involving classification of incoming packets to assign them a service path discloses the claimed instruction and criterion.

Lefebvre’s controller, as modified by Chua’s teachings, similarly discloses “receiving, by the network node from the controller, the instruction and the criterion” as recited in element 1[b]. As discussed above, Lefebvre’s traffic steering process “supports three types of service policies: subscriber-based policies, application-based policies, and flow based policies.” Lefebvre at 6:26-28. Lefebvre teaches that “[t]hese policies can be specified by the operator and pushed to the relevant switches by [the] centralized controller[,]” which a POSITA would have understood to teach receiving, by the network node (e.g., one or more of perimeter switches 102, 104, 106) from the controller, the instruction and the criterion. Chua similarly discloses the controller programs network devices “to perform programmed actions on packets” including allowing, blocking, mirroring, redirecting, transforming, and encapsulating packets. Chua at 7:28-54. Lefebvre’s controller already redirects. *See* Lefebvre at 8:49-65, Table 1, Table 2 (depicting Open-Flow switch table actions). As modified by Chua’s teachings, Lefebvre’s controller’s instructions would include the allowing, blocking, and mirroring packets.

123. Thus, the combination of Lefebvre and Chua discloses claim element [1.b].

(iv) **1[c]: receiving, by the network node from the first entity over the packet network, a packet addressed to the second entity;**

124. Lefebvre discloses claim element 1[c].

125. As discussed above for preamble 1[pre], Lefebvre states that incoming traffic “always enters the service network 100 via a perimeter switch and through a node port.” Lefebvre at 6:5-8. Lefebvre’s perimeter switches correspond to the claimed network nodes for the reasons discussed above for 1[pre]. Lefebvre discloses **user equipment 120, 122** and the **internal network 124** along with the Internet 126. Lefebvre’s **user equipment, internal network**, and Internet therefore disclose the “first and second entities.” For example, when Lefebvre’s **user equipment 120, 122** communicates with the **internal network 124** using the service network 100, the **user equipment 120, 122** discloses the first entity. Lefebvre at 5:38-54, 6:8-16. And a POSITA would have understood that in doing so, the SDN receives from the **user equipment 120, 122** a packet addressed to the second entity, **internal network 124**. Lefebvre confirms this when disclosing the source and destination address fields of the received packet. Lefebvre at 2:53-64. And similarly, Lefebvre discloses that within the network, at transit ports, packets are forwarded to their destination MAC addresses. Lefebvre at 5:65-6:12, 7:55-58.

126. Thus, Lefebvre discloses claim element 1[c].

(v) 1[d]: checking, by the network node, if the packet satisfies the criterion;

127. Lefebvre discloses claim element 1[d].

128. As discussed for claim elements 1[a]-1[b], Lefebvre discloses that the operator defines service policies specifying traffic classes and the chain of services

the traffic classes must traverse, and that the first step of traffic steering involve the classification of incoming packets. Lefebvre at 4:43-45, 6:18-19, 7:35-8:48 (describing “an example methodology for processing and classifying a packet”), FIG. 2, FIG. 5 (step 510). Lefebvre’s policies are implemented by the perimeter switches. Lefebvre at 4:43-45 (“These policies are translated by the controller into rules that are programmed on the switches in the service network. These rules steer the network traffic through the ordered chain of services as specified by the policies.”), 6:5-8 (incoming traffic “enters the service network 100 via a perimeter switch and through a node port”). And as discussed for claim elements 1[a]-1[b], Lefebvre’s classification techniques disclose the claimed criterion because they are the conditions, or basis, used to identify packets for actions. See Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions).

129. A POSITA would have understood Lefebvre’s classification of incoming packets discloses the claimed “checking, by the network node, if the packet satisfies the criterion.” Lefebvre’s classification checks the incoming packet against the claimed criterion and determines the service path the packet will traverse.

130. Thus, Lefebvre discloses claim element 1[d].

(vi) 1[e]: responsive to the packet not satisfying the criterion, sending, by the network node over the packet network, the packet to the second entity; and

131. Lefebvre discloses claim element 1[e].

132. Lefebvre states that one of its assumptions used when describing its example embodiments is that the forwarded traffic is subscriber traffic. Lefebvre at 14:23-25. As discussed for claim element 1[a], Lefebvre’s distinction between subscriber and non-subscriber traffic is one type of criterion. Lefebvre also discloses that “[f]or non-subscriber traffic, we can treat the steering network as a simple router” and can send packets using “conventional destination-IP-based forwarding.” Lefebvre at 14:25-29. Because Lefebvre’s non-subscriber traffic does not satisfy the criterion of directing subscriber traffic, the network routes the packets from their source, the claimed first entity, to their destination, the claimed second entity.

133. Thus, Lefebvre discloses claim element 1[e].

(vii) 1[f]: responsive to the packet satisfying the criterion, sending the packet, by the network node over the packet network, to an entity that is included in the instruction and is other than the second entity.

134. The combination of Lefebvre and Chua discloses claim element 1[f].

135. As discussed for claim element 1[a], Lefebvre’s classification techniques determine which service chain the traffic traverses. Lefebvre’s next destination table routes, or redirects, the packet to the appropriate service for the classification of traffic. Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions). A POSITA would have understood that Lefebvre’s services are a destination different from the intended destination of the packet. *See* Lefebvre at 15:27-46 (disclosing forwarding the packet “to the next service on the assigned

service chain” and “assigning a new destination address to the received packet in accordance with the next service to be performed”).

136. Further, as I explained in Section VII.C.1, Lefebvre’s controller modified by Chua’s teachings would include additional actions including mirroring or redirecting the packets to the service chain. Chua’s mirroring action allows the traffic and also sends a copy of the traffic for deeper inspection or recording. Chua at 7:43-45, 28:7-32. And a POSITA would have understood that both actions, mirroring and redirecting of the packets to the service chain, send the packet to an entity that is other than the second entity. As I explained in Section VII.C.1, a POSITA would have been motivated to modify Lefebvre to include these additional actions taught by Chua. And a POSITA would understand that Lefebvre’s controller, modified by Chua’s teachings, would execute DPI and therefore be the “entity that is included in the instruction,” which would also be a destination “other than the second entity.”

137. Thus, combination of Lefebvre and Chua renders obvious claim element 1[f].

3. **Claim 2: The method according to claim 1, wherein the instruction is ‘probe’, ‘mirror’, or ‘terminate’ instruction, and upon receiving by the network node the ‘terminate’ instruction, the method further comprising blocking, by the network node, the packet from being sent to the second entity and to the controller.**

138. The combination of Lefebvre and Chua renders obvious dependent claim 2.

139. As discussed for claim element 1[a], Lefebvre’s traffic steering policies include subscriber-based policies, application-based policies, and flow-based policies. Lefebvre at 6:26-31. FIG. 2 of Lefebvre depicts “an example methodology for processing and classifying a packet[.]” Lefebvre at 7:37-39.

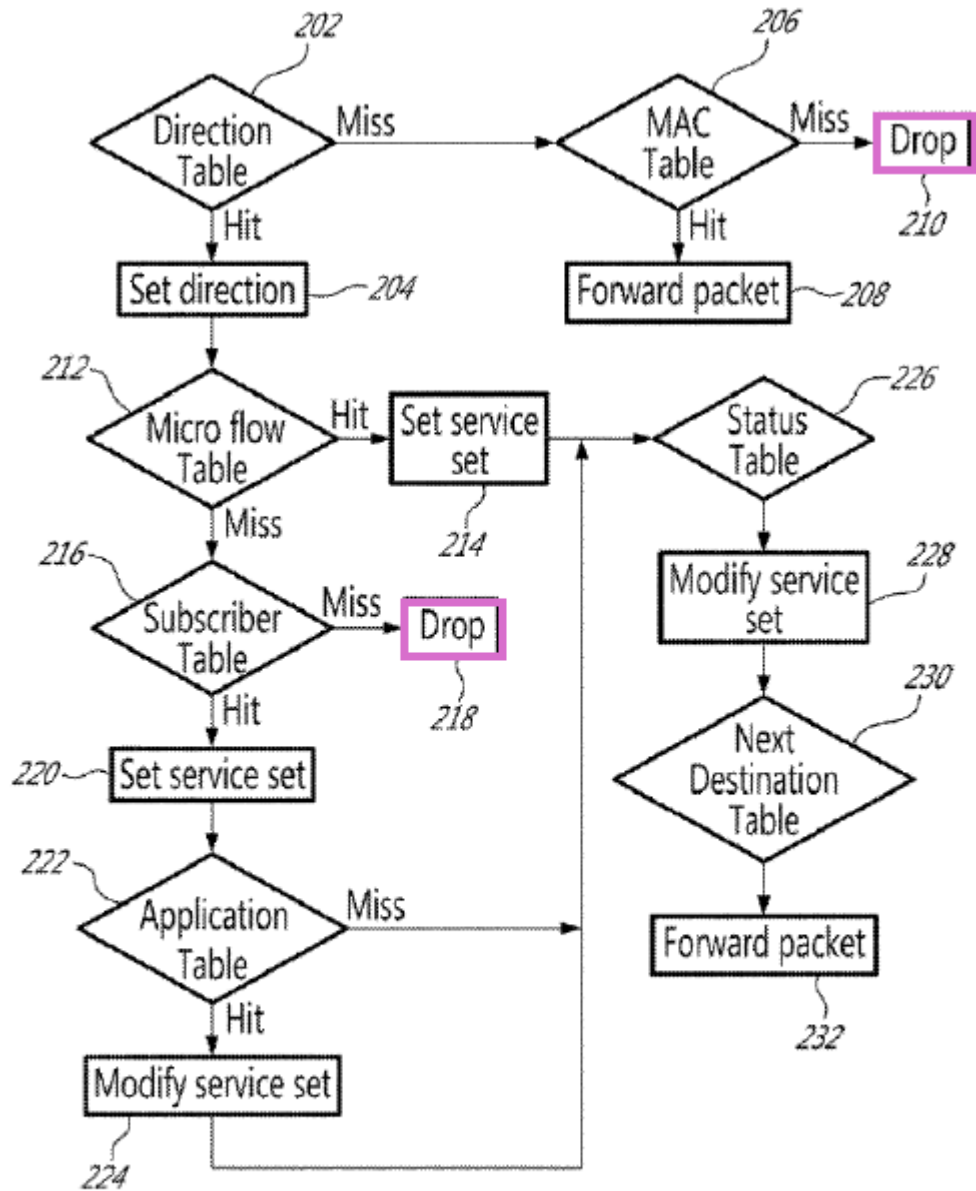


FIG. 2

Lefebvre at FIG. 2 (annotated).

140. In the example embodiments, Lefebvre discloses that when a packet arrives on a transit port, it will “miss” the direction table and proceed to the MAC table 206. Lefebvre at 7:52-54. If the packet’s destination MAC address does not

match the contents of the MAC table, Lefebvre discloses dropping the packet. Lefebvre at 7:55-58. Similarly, Lefebvre discloses “the default action is to drop the packet” when there is a miss in the subscriber table. Lefebvre at 8:11-13, FIG. 2 (step 218). Lefebvre therefore discloses dropping the packet, but Lefebvre does not explicitly disclose a terminate instruction that results in blocking, as claim 2 requires.

141. As discussed for claim element 1[a], Chua discloses the SDN controller programs network devices to perform actions including allowing, blocking, mirroring, redirecting, transforming, or encapsulating traffic. Chua at 7:35-54. Chua’s blocking action explicitly blocks the packets in the packet flow from traversing the SDN. Chua at 7:35-38, 7:41-42. Chua’s SDN controller 112 may perform these actions, including blocking, in response to information from service devices, external triggers or events, or business-level security rules. Chua at 7:28-38, 16:23-44, 28:7-32, 8:43-47, 17:26-35, 14:39-42. The combination of Lefebvre and Chua would therefore include instruction resulting in blocking, which a POSITA would have recognized as the terminate instruction required by claim 2. As discussed in Section VII.C.1, Lefebvre’s controller, as modified by Chua’s teachings, would implement Chua’s actions including blocking. See Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions); Chua at 7:33-54 (describing available actions for an SDN controller). And in doing so, the modified Lefebvre controller would provide the instruction, which Chua teaches, to the network devices

directing when to apply dropping the packet, which Lefebvre discloses. In doing so, the network devices in Lefebvre's SDN would block traffic identified by Lefebvre's controller, which executes DPI as taught by Chua. *See* Chua at 31:49-54.

142. Thus, the combination of Lefebvre and Chua renders obvious dependent claim 2.

4. **Claim 3: The method according to claim 1, wherein the instruction is a 'probe', a 'mirror', or a 'terminate' instruction, and upon receiving by the network node the 'mirror' instruction and responsive to the packet satisfying the criterion, the method further comprising sending the packet, by the network node, to the second entity and to the controller.**

143. The combination of Lefebvre and Chua renders obvious dependent claim 3.

144. Lefebvre does not disclose a mirroring instruction. But as discussed for claim element 1[a], Chua discloses the SDN controller programs network devices to perform actions including allowing, blocking, mirroring, redirecting, transforming, or encapsulating traffic. Chua at 7:28-54. Chua's mirroring action allows the traffic and also sends a copy of the traffic for deeper inspection or recording. Chua at 7:43-45, 28:7-32. Chua's SDN controller 112 may perform these actions, including mirroring, in response to information from service devices or business-level security rules. Chua at 7:28-38, 16:23-30, 16:36-44, 28:7-32, 14:39-42. And as discussed

for claim element 1[f], the combination of Lefebvre and Chua renders obvious the claimed “responsive to the packet satisfying the criterion” aspect of claim 1.

145. As discussed in Section VII.C.1, Lefebvre’s controller, as modified by Chua’s teachings, would implement Chua’s actions including mirroring. See Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions); Chua at 7:33-54 (describing available actions for an SDN controller). By doing so, a POSITA would have understood the network devices in Lefebvre’s SDN would send the packet to Lefebvre’s modified controller as well as the destination (in other words, the second entity). And Lefebvre’s controller would execute DPI, as taught by Chua. See Chua at 31:49-54.

146. The combination of Lefebvre and Chua therefore renders obvious dependent claim 3.

5. **Claim 4: The method according to claim 1, wherein the instruction is ‘probe’, ‘mirror’, or ‘terminate’ instruction, and upon receiving by the network node the ‘probe’ instruction and responsive to the packet satisfying the criterion, the method further comprising: sending the packet, by the network node, to the controller; responsive to receiving the packet, analyzing the packet, by the controller; sending the packet, by the controller, to the network node; and responsive to receiving the packet, sending the packet, by the network node, to the second entity.**

147. The combination of Lefebvre and Chua renders obvious dependent claim 4.

148. The '111 Patent discloses that the probe instruction includes matching certain aspects of a packet's header and then redirecting the packet to the controller, and matching certain other aspects of a packet's header, and then redirecting the packet to the destination. '111 Patent at 4:23-33; *see also* '111 Patent at 6:30-32, FIG. 3 (step S305).

149. Lefebvre acknowledges the need to selectively steer traffic away from expensive services, such as DPI, but does not explicitly disclose a probe instruction. *See, e.g.*, Lefebvre at 1:34-38. And Chua also doesn't explicitly disclose a probe instruction. But as discussed for claim element 1[a], Chua discloses the SDN controller programs network devices to perform actions including allowing, blocking, mirroring, redirecting, transforming, or encapsulating traffic. *See* Chua at 7:28-54. Because the claimed probe instruction involves redirects, the combination of Lefebvre and Chua renders obvious the claimed probe instruction. *See* '111 Patent at 4:23-33; *see also* '111 Patent at 6:30-32, FIG. 3 (step S305). And as discussed for claim element 1[f], the combination of Lefebvre and Chua renders obvious the claimed "responsive to the packet satisfying the criterion" aspect of claim 4.

150. Chua's redirect action sends the traffic "to another network device (such as a honeypot device or other device of service devices 116) for either inspection or to keep a potential hacker 'busy' to determine if there is a real security

threat.” Chua at 7:46-50. Because Lefebvre’s controller, modified by Chua’s teachings, executes DPI instead of a service device, the combination of Lefebvre and Chua renders obvious the claimed “sending the packet, by the network node, to the controller” and “responsive to receiving the packet, analyzing the packet, by the controller” elements of claim 4.

151. Chua discloses that if the service device deems the packets malicious, the controller may instruct the service device “to send data back to switch 210, such as data indicating whether packets of the packet flow represent a network attack and/or data of the packet flow after the data has been inspected.” Chua at 21:35-42, 28:18-32 (stating the controller “may program network devices to, in response to an indication that packets of a packet flow include malicious data, forward packets of the packet flow to a destination of the packet flow”). Chua’s SDN controller may perform these actions, including redirecting, in response to information from service devices or business-level security rules. Chua at 7:28-38, 16:23-30, 16:36-44, 28:7-32, 14:39-42. Although Chua discloses this in relation to an intrusion detection system (IDS), a POSITA would have found it obvious that service devices executing DPI would have received similar instructions. This is because IDS systems also analyze network traffic for malicious activity but typically do not employ the more rigorous inspection of packets that DPI systems use. Because Chua discloses sending data back to the network node, such as “data of the packet flow after the

data has been inspected,” the combination of Lefebvre and Chua therefore renders obvious the “sending the packet, by the controller, to the network node” element of claim 4. *See* Chua at 21:35-42, 28:18-32.

152. As discussed in Section VII.C.1, Lefebvre’s controller, as modified by Chua’s teachings, would implement Chua’s teachings regarding SDN actions, including redirecting. *See* Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions); Chua at 7:33-54 (describing available actions for an SDN controller). And as discussed in Section VII.C.1 and above, Lefebvre’s controller would execute DPI, as Chua teaches. *See* Chua at 31:49-54. As modified by Chua’s teachings, Lefebvre’s controller would instruct network devices to redirect certain traffic to the controller which would then execute DPI instead of a service device. *See* Chua at 7:46-50. Once the modified Lefebvre controller completes DPI, the controller sends the inspected packet flow back to the network device for transmission onward to the second entity, as Chua teaches. *See* Chua at 21:35-42, 28:18-32 (stating the controller “may program the network devices to, in response to an indication that packets of a packet flow include malicious data, forward packets of the packet flow to a destination of the packet flow”). This renders obvious “responsive to receiving the packet, sending the packet, by the network node, to the second entity” element of claim 4.

153. Accordingly, the combination of Lefebvre and Chua renders obvious dependent claim 4.

6. Claim 5: The method according to claim 1, further comprising responsive to the packet satisfying the criterion and to the instruction, sending the packet or a portion thereof, by the network node, to the controller.

154. The combination of Lefebvre and Chua renders obvious dependent claim 5.

155. As discussed for claim element 1[f], the combination of Lefebvre and Chua renders obvious the “responsive to the packet satisfying the criterion” aspect of claim 5.

156. As discussed in Section VII.C.1, Lefebvre’s controller, as modified by Chua’s teachings, would implement Chua’s actions including redirecting. *See* Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions); Chua at 7:33-54 (describing available actions for an SDN controller). And Lefebvre’s controller would execute DPI, as taught by Chua. *See* Chua at 31:49-54. So, as modified by Chua’s teachings, Lefebvre’s controller would instruct network devices to redirect certain traffic to the controller which would then execute DPI. And because Lefebvre contemplates steering entire packets, the modified Lefebvre controller would continue to redirect the entire packet. Lefebvre at 6:17-31; *see also* Lefebvre at 1:28-38 (discussing DPI).

157. The combination of Lefebvre and Chua therefore renders obvious dependent claim 5.

7. Claim 6: The method according to claim 5, further comprising storing the received packet or a portion thereof, by the controller, in memory.

158. The combination of Lefebvre and Chua renders obvious dependent claim 6.

159. As discussed above for Claim 5, in the combined system, Lefebvre's controller would execute DPI, as taught by Chua. *See* Chua at 31:49-54. So, as modified by Chua's teachings, Lefebvre's controller would instruct network devices to redirect certain traffic to the controller which would then execute DPI.

160. As shown in FIG. 1 of Chua, SDN controller is remote from network devices 108 and 100. Chua at Fig. 1. Chua states that "SDN controller 112 may inspect one or more preliminary packets of packet flows originating from or directed to client device 102, and after determining that the packet flows are not malicious (after a predetermined number of packets), stop inspecting the packet flows." Chua at 31:50-54. A POSITA would have understood from this excerpt from Chua that, in order to determine that SDN controller 112 has inspected a predetermined number of packets belonging to the same packet flow, SDN controller 112 must store at the very least certain indicator(s) that can identify the packet flow, e.g., flow identifier, which would be a portion of the packet header.

161. Although Lefebvre omits detailed discussion of its controller, it is my opinion that a POSITA would recognize that Lefebvre's controller includes components including processors and memory. For example, Lefebvre discloses that embodiments of what it describes may exist as a software product executing programs. Lefebvre at 17:17-37. This confirms that a POSITA would recognize that Lefebvre's controller includes components including processors and memory. Moreover, Chua confirms how controllers include a control unit with "one or more processors and/or computer readable memory for storing software or firmware instructions." Chua at 10:67-11:6, 31:60-32:6.

162. It would have been obvious to a POSITA that the process of Lefebvre's modified controller executing DPI on a received packet would involve storing the received packet, by the controller, in memory as claimed. As I discussed above, DPI is a content-based technique that inspects both the header and the payload of a packet to classify network traffic. '111 Patent at 1:21-29 (describing DPI as one type of dedicated service); Liao at 1. DPI relies on patterns or signatures contained in payloads for network applications. A POSITA would have understood that the received packet would be stored in some form of memory by the controller in order to permit the controller to perform DPI. I note that claim 6 does not specify any particular type of memory in which the packet must be stored.

163. The combination of Lefebvre and Chua therefore renders obvious dependent claim 6.

8. Claim 9: The method according to claim 5, further comprising responsive to receiving the packet, analyzing the packet, by the controller.

164. The combination of Lefebvre and Chua renders obvious dependent claim 9.

165. As discussed for claim 5, Lefebvre's controller, as modified by Chua's teachings, would implement Chua's actions including redirecting. *See* Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions); Chua at 7:33-54 (describing available actions for an SDN controller). And Lefebvre's controller would execute DPI, as taught by Chua. *See* Chua at 31:49-54. So, as modified by Chua's teachings, Lefebvre's controller would instruct network devices to redirect certain traffic to the controller which would then execute DPI. And because Lefebvre contemplates steering entire packets, the modified Lefebvre controller would continue to redirect the entire packet. Lefebvre at 6:17-31; *see also* Lefebvre at 1:28-38 (discussing DPI). A POSITA would have understood that the DPI performed by the modified Lefebvre controller involves "analyzing the packet" as claimed. *See, e.g.,* Liao at 2 ("DPI technique inspects both the header and the payload of a packet.").

166. The combination of Lefebvre and Chua therefore renders obvious dependent claim 9.

9. Claim 10: The method according to claim 9, further for use with an application server that communicates with the controller, wherein the analyzing comprising sending the packet, by the controller, to the application server, and analyzing the packet by the application server.

167. The combination of Lefebvre and Chua renders obvious dependent claim 10.

168. Claim 10 recites an “application server.” The ’111 Patent describes that “[a]n application server 120 executes, for example, security applications (e.g., Firewall, intrusion detection, etc.), data analytic applications, and so on.” ’111 Patent at 3:56-61.

169. As discussed above for claims 5 and 9, Lefebvre’s controller, modified by Chua’s teachings, executes DPI instead of a service device. Accordingly, the combination of Lefebvre and Chua renders obvious the claimed “sending the packet or a portion thereof, by the network node, to the controller” and “responsive to receiving the packet, analyzing the packet, by the controller” elements of claims 5 and 9.

170. Chua further teaches that its controller sends the packet to other devices based on the DPI. For instance, Chua discloses that certain types of traffic “must often be distributed to a variety of appliances or server-based application-aware

devices based on potentially deep inspection of incoming (and for certain flow types, outgoing) packets.” Chua at 15:5-9; *see also* Chua at 15:9-17 (“Rather than route all traffic through L4-L7 firewalls or application load balancers, or utilize distributed protocols such as policy based routing with limited capability and complex network interactions, SDN controller 112 may allow customers (e.g., administrator 114) to directly sort traffic on a per-packet or per-flow basis for individualized processing, saving cost, improving performance, limiting risk, improving availability, and increasing control.”). Chua’s appliances or server-based application-aware devices correspond to the claimed “application server that communicates with the controller.” Chua’s disclosure that traffic is distributed to appliances or server-based application-aware devices based on DPI (performed by Chua’s controller) teaches sending the packet, by the controller, to the application server as claimed.

171. A POSITA would have understood that packets sent to the appliances or server-based application-aware devices based on DPI would be analyzed, which teaches “analyzing the packet by the application server” as claimed. Chua teaches that these devices provide security applications consistent with the description in the ’111 Patent. ’111 Patent at 3:56-61 (’111 Patent describing that “an application server 120 executes, for example, security applications (e.g., Firewall, intrusion detection, etc.), data analytic applications, and so on.”). For example, Chua

discloses that SDN controller 218 may determine that a particular packet flow should be inspected for intrusion detection. *See* Chua at 21:35-37.

172. Accordingly, the combination of Lefebvre and Chua renders obvious dependent claim 10.

10. Claim 11: The method according to claim 10, wherein the analyzing further comprising sending the packet after analyzing by the application server to the controller, and sending the packet, after receiving from the controller by the network node, to the second entity.

173. The combination of Lefebvre and Chua renders obvious dependent claim 11.

174. As discussed for claim 10, Chua teaches that its controller sends a packet to an application server for analysis (e.g., for intrusion detection) based on DPI. Furthermore, Chua discloses that the controller may instruct the service device “to send data back to switch 210, such as data indicating whether packets of the packet flow represent a network attack and/or data of the packet flow after the data has been inspected.” Chua at 21:35-42, 28:18-32 (stating the controller “may program the network devices to, in response to an indication that packets of a packet flow include malicious data, forward packets of the packet flow to a destination of the packet flow.”). Because Chua also teaches that the controller can send packets to service devices for analysis, a POSITA would have understood Chua’s teaching of sending data (e.g., data indicating whether packets of the packet flow represent a

network attack and/or data of the packet flow after the data has been inspected) would also be applicable to scenarios in which the controller sends a packet to a service device (e.g., in the case of Chua's controller distributing traffic to an appliance or server-based application-aware device, such as intrusion detection, based on deep inspection). Chua at 15:5-17, 21:35-37. Because Chua discloses sending data back, such as "data of the packet flow after the data has been inspected," the combination of Lefebvre and Chua therefore renders obvious the "sending the packet after analyzing by the application server to the controller" element of claim 11. *See* Chua at 21:35-42, 28:18-32.

175. As discussed in Section VII.C.1, Lefebvre's controller, as modified by Chua's teachings, would implement Chua's teachings regarding SDN actions, including redirecting. *See* Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions); Chua at 7:33-54 (describing available actions for an SDN controller). As discussed above, as modified by Chua's teachings, Lefebvre's controller would redirect certain traffic to an application server for analysis (e.g., intrusion detection) based on the DPI. *See* Chua at 15:5-17. Once the application server completes the analysis (e.g., intrusion detection), the application server sends the packet to the modified Lefebvre controller, which sends the inspected packet flow back to the network device for transmission onward to the second entity, as Chua teaches. *See* Chua at 21:35-42, 28:18-32 (stating the

controller “may program the network devices to, in response to an indication that packets of a packet flow include malicious data, forward packets of the packet flow to a destination of the packet flow.”). This renders obvious “sending the packet, after receiving from the controller by the network node, to the second entity” element of claim 11.

11. Claim 12: The method according to claim 9, wherein the analyzing comprises applying security or data analytic application.

176. The combination of Lefebvre and Chua renders obvious dependent claim 12.

177. As discussed for claim 9, a POSITA would have understood that the DPI performed by the modified Lefebvre controller involves “analyzing the packet” as recited in claim 9. A POSITA would have understood that DPI is one example of “applying security or data analytic application” as claimed. *See, e.g.*, Chua at 31:48-54 (“In some examples, SDN controller 112 further performs deep packet inspection (DPI) on packets from client device 102 (402). For example, SDN controller 112 may inspect one or more preliminary packets of packet flows originating from or directed to client device 102, and after determining that the packet flows are not malicious (after a predetermind number of packets), stop inspecting the packet flows.”).

178. Additionally, Chua discloses that “[s]ervice devices 116 may include, for example, intrusion detection service (IDS) devices, intrusion prevention system (IPS) devices, web proxies, web servers, web-application firewalls and the like.” Chua at 5:59-62. Other examples of service devices 116 include “devices for providing services such as, for example, denial of service (DoS) protection, distributed denial of service (DDoS) protection, traffic filtering, wide area network (WAN) acceleration, or other such services” as well as “malware detection devices, network anti-virus devices, network packet capture and analysis devices, honeypot devices, reflector net devices, tar pit devices, domain name service (DNS) and global DNS server devices, mail proxies, and anti-spam devices.” Chua at 5:62-6:5. Chua explains that service devices 116 are examples of “L4-L7 devices” (Chua at 14:39-42) and further discloses that “SDN controller itself may host one or more L4-L7 services, rather than (or in addition to) services provided by service devices 116.” Chua at 6:42-45. Such services, when performed by the SDN controller, constitute further examples of “applying security or data analytic application” as claimed.

179. The combination of Lefebvre and Chua therefore renders obvious dependent claim 12.

12. Claim 13: The method according to claim 9, wherein the analyzing comprises applying security application that comprises firewall or intrusion detection functionality.

180. The combination of Lefebvre and Chua renders obvious dependent claim 13.

181. As discussed for claim 12, Chua discloses “SDN controller itself may host one or more L4-L7 services, rather than (or in addition to) services provided by service devices 116.” Chua at 6:42-45. Those services include, for example, “intrusion detection service (IDS)” and “firewalls.” Chua at 5:59-62; *see also* Chua at 14:39-42 (service devices 116 are examples of “L4-L7 devices”). As discussed above in Section VII.C.1, it would have been obvious to modify Lefebvre’s controller to provide such services. Such services as “intrusion detection service (IDS)” and “firewalls,” when performed by the SDN controller, render obvious “wherein the analyzing comprises applying security application that comprises firewall or intrusion detection functionality” as claimed.

182. Accordingly, the combination of Lefebvre and Chua renders obvious dependent claim 13.

13. Claim 14: The method according to claim 9, wherein the analyzing comprises performing Deep Packet Inspection (DPI) or using a DPI engine on the packet.

183. The combination of Lefebvre and Chua renders obvious dependent claim 5.

184. As discussed for above for claims 5 and 9, Lefebvre's controller, as modified by Chua's teachings, would implement Chua's actions including redirecting. See Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions); Chua at 7:33-54 (describing available actions for an SDN controller). And Lefebvre's controller would execute DPI, as taught by Chua. See Chua at 31:49-54. So, as modified by Chua's teachings, Lefebvre's controller would instruct network devices to redirect certain traffic to the controller which would then execute DPI. Thus, the combination renders obvious "wherein the analyzing comprising performing Deep Packet Inspection (DPI) or using a DPI engine on the packet" as claimed.

185. Accordingly, the combination of Lefebvre and Chua renders obvious dependent claim 14.

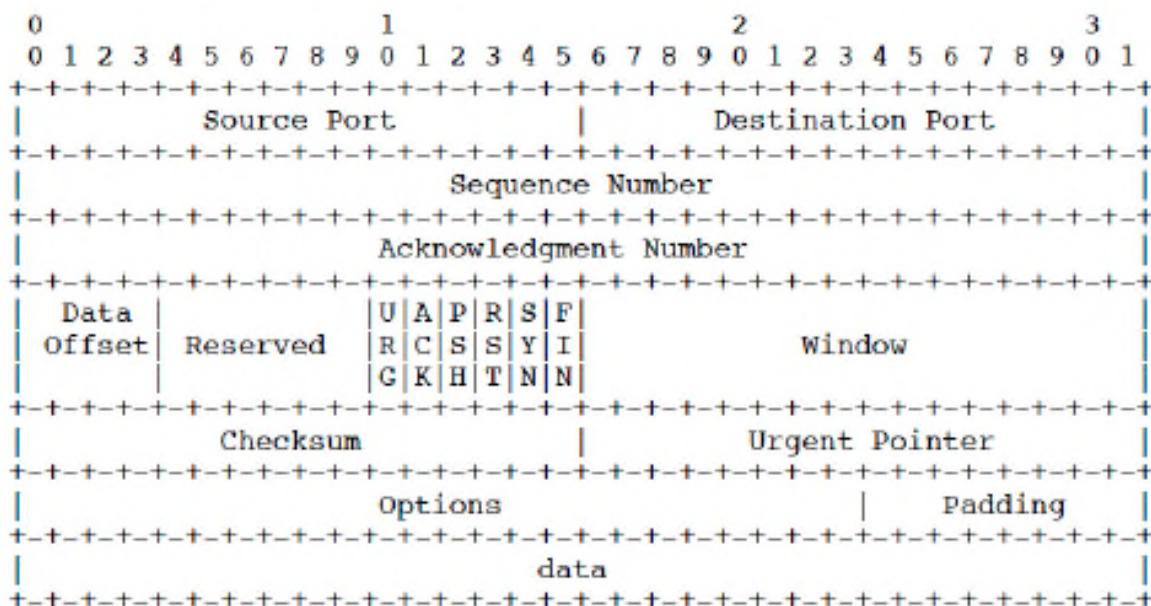
14. Claim 15: The method according to claim 9, wherein the packet comprises distinct header and payload fields, and wherein the analyzing comprises checking part of, or whole of, the payload field.

186. The combination of Lefebvre and Chua renders obvious dependent claim 15.

187. A POSITA would have understood that a packet comprises distinct header and payload fields. For example, a POSITA would have understood that Transmission Control Protocol (TCP) packets include separate and distinct header and payload fields. RFC 793, published September 1981, defines TCP. See

EX1015, RFC 793 (“RFC 793”); *see also* Liao at 1 (“A packet is composed with header and payload, and the header carries layering information, such as the IP address is in the layer three and the port number is in the layer four. The payload carries upper layer application protocol and data.”). I have reproduced below Figure 3 of RFC 793 which depicts the TCP header format.

TCP Header Format



TCP Header Format

Note that one tick mark represents one bit position.

Figure 3.

188. As discussed above for claim 14, Lefebvre’s controller, as modified by Chua’s teachings, would implement Chua’s actions including redirecting. *See* Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions); Chua at 7:33-54 (describing available actions for an SDN controller). And

Lefebvre's controller would execute DPI, as taught by Chua. *See* Chua at 31:49-54. So, as modified by Chua's teachings, Lefebvre's controller would instruct network devices to redirect certain traffic to the controller which would then execute DPI. Well before the assumed April 22, 2014 priority date of the '111 Patent, a POSITA would have been aware that DPI analysis involves checking part of, or whole of, the payload field of a packet. As previously explained in Section VI.A, a POSITA would have understood that DPI is a content-based technique that inspects both the header and the payload of a packet to classify network traffic. *See also* Liao at 2 ("DPI technique inspects both the header and the payload of a packet."). Thus, when Lefebvre's modified controller performs DPI, this teaches "wherein the analyzing comprises checking part of, or whole of, the payload field" as claimed.

189. Accordingly, the combination of Lefebvre and Chua renders obvious dependent claim 15.

- 15. Claim 18: The method according to claim 1, wherein the packet comprises distinct header and payload fields, the header comprises at least the first and second entities addresses in the packet network, and wherein the packet-applicable criterion is that the first entity address, the second entity address, or both match a predetermined address or addresses.**

190. The combination of Lefebvre and Chua renders obvious dependent claim 18.

191. A POSITA would have understood that IP packets include separate and distinct header and payload fields. See EX1008, 1 (“A packet is composed with header and payload[.]”); RFC 793 at 15 (describing “Internet Protocol header”). And a POSITA would have understood that IP packets include source and destination addresses. See RFC 793 at 15 (“The Internet Protocol header carries several information fields, including the source and destination host addresses.”).

192. Confirming this, Lefebvre discloses associating a service set based on the direction of the packet and the header fields of packets including the “source address, a destination address, a source port, a destination port and a protocol.” Lefebvre at 2:47-52, 7:59-67, 8:4-30. The source and destination addresses Lefebvre discloses matching against in the header fields are the claimed first and second entities’ addresses in the packet network, and the addresses Lefebvre uses to identify the matching packets are the claimed predetermined addresses.

193. The combination of Lefebvre and Chua therefore renders obvious dependent claim 18.

16. Claim 19: The method according to claim 18, wherein the addresses are Internet Protocol (IP) addresses.

194. The combination of Lefebvre and Chua renders obvious dependent claim 19.

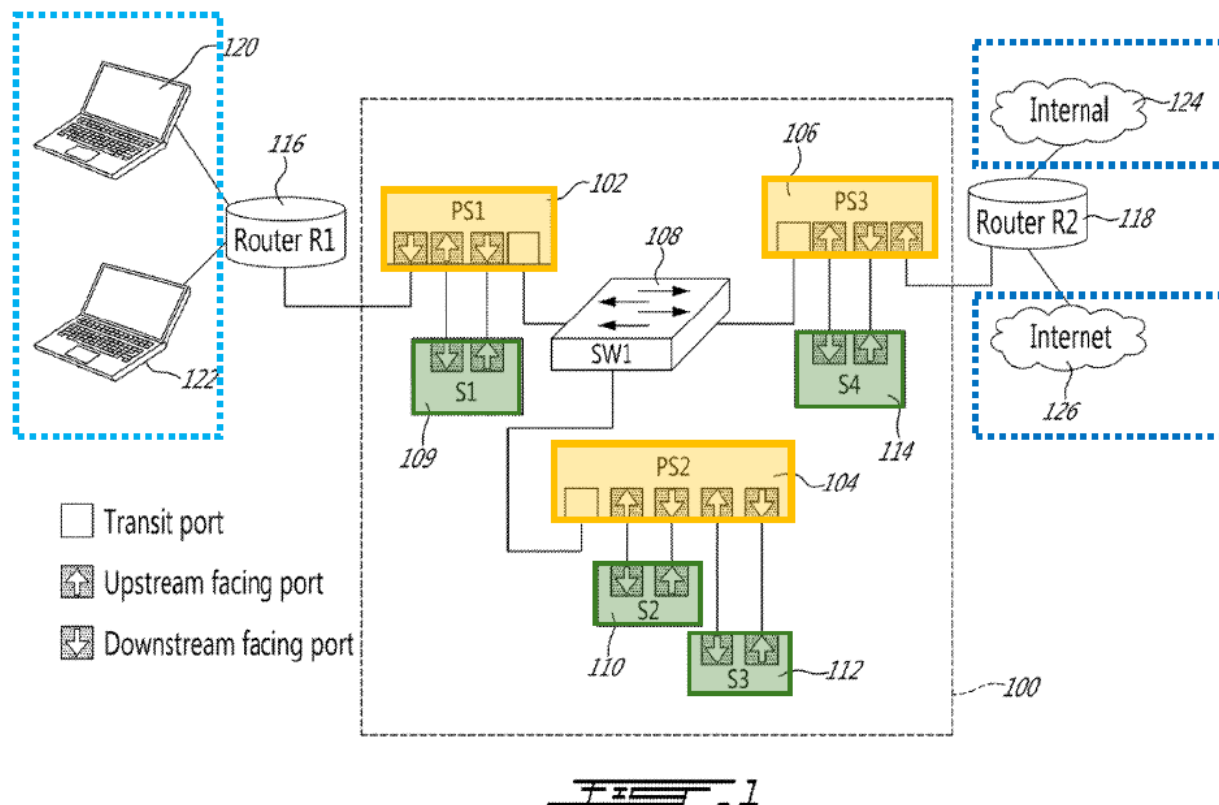
195. As discussed for claim 18, IP packets include source and destination addresses. A POSITA would have understood these addresses are IP addresses.

196. The combination of Lefebvre and Chua therefore renders obvious dependent claim 19.

17. Claim 21: The method according to claim 1, wherein the packet network comprises a Wide Area Network (WAN), Local Area Network (LAN), the Internet, Metropolitan Area Network (MAN), Internet Service Provider (ISP) backbone, datacenter network, or inter-datacenter network.

197. The combination of Lefebvre and Chua renders obvious dependent claim 21.

198. As shown in annotated Figure 1 of Lefebvre below, Lefebvre discloses that the network includes **user equipment 120, 122** connected to router R1 and the **internal network 124** and the **Internet 126** connected to router R2. Lefebvre at 5:38-54, 6:13-16. A POSITA would therefore understand that Lefebvre's service network is at least a LAN if not a WAN. And Lefebvre's service network includes Internet 126.



Lefebvre at FIG. 1 (annotated).

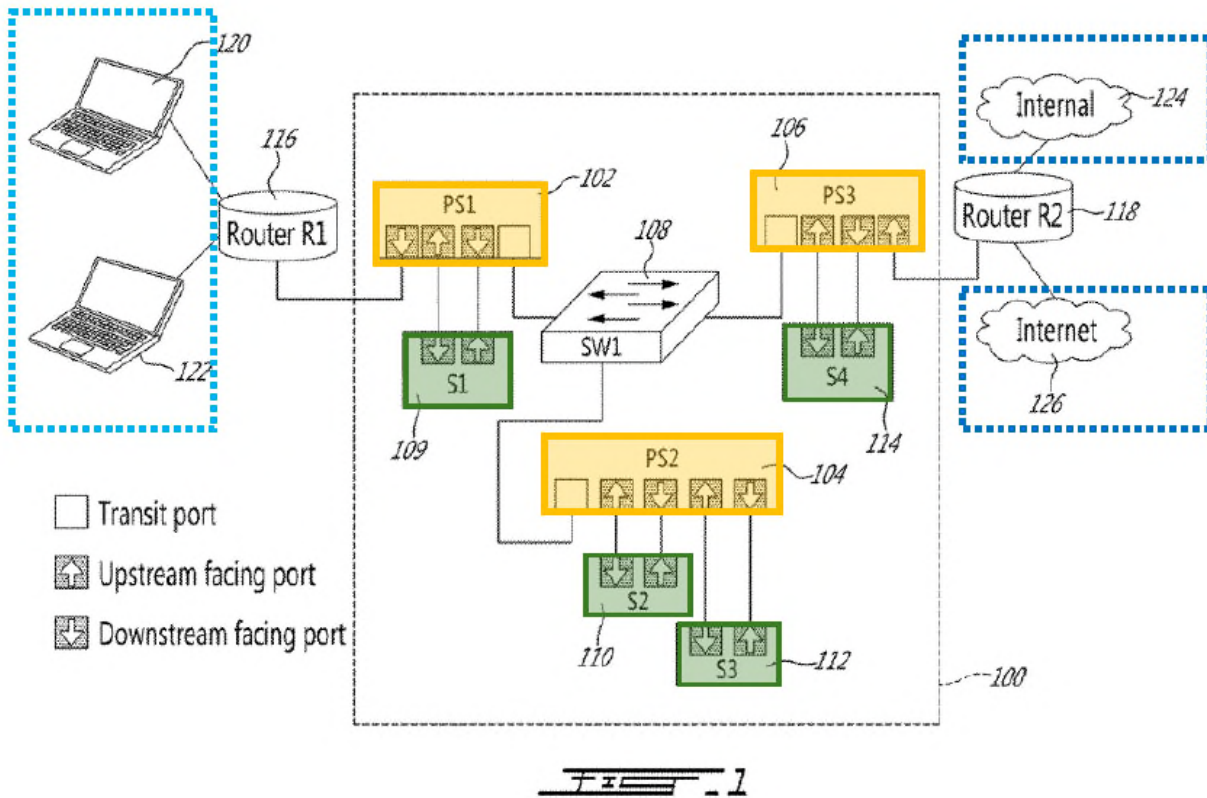
199. The combination of Lefebvre and Chua therefore renders obvious dependent claim 21.

18. Claim 22: The method according to claim 1, wherein the first entity is a server device and the second entity is a client device, or wherein the first entity is a client device and the second entity is a server device.

200. The combination of Lefebvre and Chua renders obvious dependent claim 22.

201. As shown in annotated Figure 1 of Lefebvre below, Lefebvre discloses that the network includes **user equipment 120, 122** connected to router R1 and the

internal network 124 and the Internet 126 connected to router R2. Lefebvre at 5:38-54, 6:13-16. A POSITA would therefore understand that Lefebvre’s user equipment 120, 122 are client devices. And a POSITA would understand that the internal network 124 and the Internet 126 include servers. See, e.g., Moore at 11 (describing the detection of web servers operating on non-standard ports on an internal network); Chua at 5:51-53 (describing that an SDN “may provide services to network traffic flowing between client device 102 and server device 104”).



202. The combination of Lefebvre and Chua therefore renders obvious dependent claim 22.

19. **Claim 23: The method according to claim 22, wherein the server device comprises a web server, and wherein the client device comprises a smartphone, a tablet computer, a personal computer, a laptop computer, or a wearable computing device.**

203. The combination of Lefebvre and Chua renders obvious dependent claim 23.

204. As discussed for claim 22, Lefebvre discloses a service network including **user equipment 120, 122** connected to router R1 and the **internal network 124** and the **Internet 126** connected to router R2. Lefebvre at 5:38-54, 6:13-16. And Lefebvre depicts **user equipment 120, 122** as laptops. Lefebvre at FIG. 1. A POSITA would therefore understand that Lefebvre's **user equipment 120, 122** are client devices which could include a smartphone, tablet computer, personal computer, laptop computer, or wearable computing device as claimed. And a POSITA would understand that the **internal network 124** and the **Internet 126** include servers, like web servers. See Moore at 11 (describing the detection of web servers operating on non-standard ports on an internal network).

205. The combination of Lefebvre and Chua therefore renders obvious dependent claim 23.

20. Claim 24: The method according to claim 22, wherein the communication between the network node and the controller is based on, or uses, a standard protocol.

206. The combination of Lefebvre and Chua renders obvious dependent claim 24.

207. Lefebvre discloses that its SDN use the OpenFlow protocol. Lefebvre at 4:30-40. As Lefebvre discloses, “OpenFlow is a communications protocol that gives access to the forwarding plane of a network switch or router over the network.” Lefebvre at 4:33-35. Chua confirms this when disclosing that OpenFlow is an open protocol for implementing software defined networking. Chua at 1:35-41; *see also* McKeown.

208. The Open Networking Foundation (ONF) manages the OpenFlow protocol and related technologies. *See, e.g.,* EX1016, 2 (“ONF community standardized the OpenFlow protocol to enable separation of the network control and data planes, thus enabling multi-vendor SDN implementations.”). A POSITA would have therefore understood the OpenFlow protocol is a standard protocol.

209. The combination of Lefebvre and Chua therefore renders obvious dependent claim 24.

21. Claim 25: The method according to claim 24, wherein the standard protocol is according to, based on, or compatible with, an OpenFlow protocol version 1.3.3 or 1.4.0.

210. The combination of Lefebvre and Chua renders obvious dependent claim 25.

211. As discussed for claim 24, the ONF manages the OpenFlow protocol and related technologies. *See, e.g.*, EX1016, 2 (“ONF community standardized the OpenFlow protocol to enable separation of the network control and data planes, thus enabling multi-vendor SDN implementations.”). Lefebvre discloses that its SDN uses certain features from version 1.1 of the OpenFlow protocol. Lefebvre at 4:30-40.

212. The ONF published version 1.3.3 of the OpenFlow protocol in September 2013. EX1017, 3. And the ONF published version 1.4.0 of the OpenFlow protocol on October 14, 2013. EX1017, 3; *see also* EX1018. To the extent that OpenFlow 1.1 is not compatible with OpenFlow protocol version 1.3.3 and 1.4.0, a POSITA would have found it obvious to modify Lefebvre’s SDN for compatibility, or to be based on, OpenFlow protocol version 1.3.3 or 1.4.0.

213. The combination of Lefebvre and Chua therefore renders obvious dependent claim 25.

22. Claim 26: The method according to claim 25, wherein the instruction comprises a Type-Length-Value (TLV) structure.

214. The combination of Lefebvre and Chua renders obvious dependent claim 26.

215. Type-length-value (TLV) structures are well known data structures often used in protocols. For example, RFC 5810, published March 2010, discloses that the ForCES protocol makes extensive use of TLVs. EX1019 (RFC 5810, available at <https://www.rfc-editor.org/rfc/rfc5810.html>). And OpenFlow protocol version 1.4.0, published October 14, 2013, makes use of TLVs. *See, e.g.*, EX1018 at 52. A POSITA would have therefore found it obvious to modify Lefebvre's SDN to utilize instructions with a TLV structure.

216. The combination of Lefebvre and Chua therefore renders obvious dependent claim 26.

23. Claim 27: The method according to claim 1, wherein the network node comprises a router, a switch, or a bridge.

217. The combination of Lefebvre and Chua renders obvious dependent claim 27.

218. Lefebvre discloses a service network as shown in annotated FIG. 1 below.

24. Claim 28: The method according to claim 1, wherein the packet network is an Internet Protocol (IP) network, and the packet is an IP packet.

221. The combination of Lefebvre and Chua renders obvious dependent claim 28.

222. Lefebvre's traffic steering process contemplates service policies defined by IP address blocks and IP addresses, for example. *See, e.g.*, Lefebvre at 6:38-41, 6:46-48, 7:60-66. A POSITA would have therefore understood Lefebvre's packet network is an IP network.

223. The combination of Lefebvre and Chua therefore renders obvious dependent claim 28.

25. Claim 29: The method according to claim 28, wherein the packet network is an Transmission Control Protocol (TCP) network, and the packet is an TCP packet.

224. The combination of Lefebvre and Chua renders obvious dependent claim 29.

225. Lefebvre's traffic steering process contemplates service policies defined by TCP source and destination ports and TCP/UDP flows, for example. Lefebvre at 6:38-41, 7:60-66. A POSITA would have therefore understood Lefebvre's packet network is a TCP network with TCP packets.

226. The combination of Lefebvre and Chua therefore renders obvious dependent claim 29.

26. Claim 30: The method according to claim 1, further comprising: receiving, by the network node from the first entity over the packet network, one or more additional packets; checking, by the network node, if any one of the one or more additional packets satisfies the criterion; responsive to an additional packet not satisfying the criterion, sending, by the network node over the packet network, the additional packet to the second entity; and responsive to the additional packet satisfying the criterion, sending the additional packet, by the network node over the packet network, in response to the instruction.

227. The combination of Lefebvre and Chua renders obvious dependent claim 30.

228. Lefebvre discloses steering packet traffic, which a POSITA would have understood discloses the required “receiving, by the network node from the first entity over the packet network, one or more additional packets.” Lefebvre at 2:30-38. As discussed for claim element 1[a], Lefebvre discloses flow-based policies. A POSITA would have understood this discloses “checking, by the network node, if any one of the one or more additional packets satisfies the criterion” because they apply to flows, which are one or more additional packets. Lefebvre at 6:46-53. As discussed for claim element 1[e], Lefebvre’s non-subscriber traffic does not satisfy the criterion of directing subscriber traffic so the packets are routed to the destination. See Lefebvre at 14:25-29. A POSITA would have understood this discloses “responsive to an additional packet not satisfying the criterion, sending by the network node over the packet network, the additional packet to the second

entity.” And Lefebvre discloses how multiple packets are “processed and steered” to the next node in their assigned service paths. Lefebvre at 6:5-12, 6:17-25. A POSITA would have therefore understood Lefebvre discloses “responsive to the additional packet satisfying the criterion, sending the additional packet, by the network node over the packet network, in response to the instruction.”

229. The combination of Lefebvre and Chua therefore renders obvious dependent claim 30.

27. Claim 31: The method according to claim 1, wherein the packet network is a Software Defined Network (SDN), the packet is routed as part of a data plane and the network node communication with the controller serves as a control plane.

230. The combination of Lefebvre and Chua renders obvious dependent claim 31.

231. Lefebvre discloses that its service network is a software defined network (SDN). See Lefebvre at 4:30-40. A POSITA would have understood that in an SDN, the packets are routed as part of the data plane and that communication with the controller serves as the control plane. See, e.g., EX1011 at 2; Chua at 1:46-52 (“A software defined network is generally a network of interconnected computing devices having forwarding planes or data planes that can be programmed remotely by one or more controller devices. In this manner, the control plane can be physically separate from the data plane (or forwarding plane) for an SDN.”).

232. The combination of Lefebvre and Chua therefore renders obvious dependent claim 31.

28. Claim 32

233. Independent claim 32 is substantially similar to claim 1 above. The primary difference is that claim 32 recites a “method by the network node.” It is my opinion that Lefebvre in view of Chua renders obvious independent claim 32 for substantially the same reasons as discussed above for independent claim 1.

(i) 32[pre]: A method for use with a packet network including a network node for transporting packets between first and second entities under control of a controller that is external to the network node, the method by the network node comprising:

234. If the preamble is limiting, the combination of Lefebvre and Chua renders obvious preamble 32[pre].

235. Preamble 32[pre] is similar to preamble 1[pre] addressed above, which recites “[a] method for use with a packet network including a network node for transporting packets between first and second entities under control of a controller that is external to the network node, the method comprising[.]” Thus, the combination of Lefebvre and Chua renders obvious preamble 32[pre] for the same reasons discussed above for preamble 1[pre].

(ii) 32[a]: receiving, from the controller, the instruction and the criterion;

236. The combination of Lefebvre and Chua renders obvious claim element 32[a].

237. Claim element 32[a] is substantially the same as claim element 1[b] addressed above, which recites “receiving, by the network node from the controller, the instruction and the criterion[.]” Thus, the combination of Lefebvre and Chua renders obvious claim element 32[a] for the same reasons discussed above for claim elements 1[a]-1[b].

(iii) 32[b]: receiving, from the first entity over the packet network, a packet addressed to the second entity;

238. Lefebvre discloses claim element 32[b].

239. Claim element 32[b] is substantially the same as claim element 1[c] addressed above, which recites “receiving, by the network node from the first entity over the packet network, a packet addressed to the second entity[.]” Thus, the combination of Lefebvre and Chua renders obvious claim element 32[b] for the same reasons discussed above for claim element 1[c].

(iv) 32[c]: checking if the packet satisfies the criterion;

240. The combination of Lefebvre and Chua renders obvious claim element 32[c].

241. Claim element 32[c] is substantially the same as claim element 1[d] addressed above, which recites “checking, by the network node, if the packet

satisfies the criterion[.]” Thus, the combination of Lefebvre and Chua renders obvious claim element 32[c] for the same reasons discussed above for claim element 1[d].

(v) 32[d]: responsive to the packet not satisfying the criterion, sending over the packet network, the packet to the second entity; and

242. The combination of Lefebvre and Chua renders obvious claim element 32[d].

243. Claim element 32[d] is substantially the same as claim element 1[e] addressed above, which recites “responsive to the packet not satisfying the criterion, sending, by the network node over the packet network, the packet to the second entity[.]” Thus, the combination of Lefebvre and Chua renders obvious claim element 32[d] for the same reasons discussed above for claim element 1[e].

(vi) 32[e]: responsive to the packet satisfying the criterion, sending the packet over the packet network, to an entity that is included in the instruction and is other than the second entity.

244. The combination of Lefebvre and Chua renders obvious claim element 32[e].

245. Claim element 32[e] is substantially the same as claim element 1[f] addressed above, which recites “responsive to the packet satisfying the criterion, sending the packet, by the network node over the packet network, to an entity that is included in the instruction and is other than the second entity.” Thus, the

combination of Lefebvre and Chua renders obvious claim element 32[e] for the same reasons discussed above for claim element 1[f].

29. Claim 33: The method according to claim 32, wherein the instruction is ‘probe’, ‘mirror’, or ‘terminate’ instruction, and upon receiving the ‘terminate’ instruction, the method further comprising blocking, the packet from being sent to the second entity and to the controller.

246. The combination of Lefebvre and Chua renders obvious claim 33.

247. Claim 33 is substantially the same as claim 2 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 33 for the same reasons discussed above for claim 2.

30. Claim 34: The method according to claim 32, wherein the instruction is a ‘probe’, a ‘mirror’, or a ‘terminate’ instruction, and upon receiving the ‘mirror’ instruction and responsive to the packet satisfying the criterion, the method further comprising sending the packet to the second entity and to the controller.

248. The combination of Lefebvre and Chua renders obvious claim 34.

249. Claim 34 is substantially the same as claim 3 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 34 for the same reasons discussed above for claim 3.

31. Claim 35: The method according to claim 32, wherein the instruction is ‘probe’, ‘mirror’, or ‘terminate’ instruction, and upon receiving the ‘probe’ instruction and responsive to the packet satisfying the criterion, the method further comprising: sending the packet to the controller; receiving the packet, from the controller; and responsive to receiving the packet, sending the packet, to the second entity.

250. The combination of Lefebvre and Chua renders obvious claim 35.

251. Claim 35 is substantially the same as claim 4 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 35 for the same reasons discussed above for claim 4.

32. Claim 36: The method according to claim 32, further comprising responsive to the packet satisfying the criterion and to the instruction, sending the packet or a portion thereof to the controller.

252. The combination of Lefebvre and Chua renders obvious claim 36.

253. Claim 36 is substantially the same as claim 5 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 36 for the same reasons discussed above for claim 5.

33. Claim 41: The method according to claim 32, wherein the packet comprises distinct header and payload fields, the header comprises at least the first and second entities addresses in the packet network, and wherein the packet-applicable criterion is that the first entity address, the second entity address, or both match a predetermined address or addresses.

254. The combination of Lefebvre and Chua renders obvious claim 41.

255. Claim 41 is substantially the same as claim 18 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 41 for the same reasons discussed above for claim 18.

34. Claim 42: The method according to claim 41, wherein the addresses are Internet Protocol (IP) addresses.

256. The combination of Lefebvre and Chua renders obvious claim 42.

257. Claim 42 is substantially the same as claim 19 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 42 for the same reasons discussed above for claim 19.

35. Claim 44: The method according to claim 32, wherein the packet network comprises a Wide Area Network (WAN), Local Area Network (LAN), the Internet, Metropolitan Area Network (MAN), Internet Service Provider (ISP) backbone, datacenter network, or inter-datacenter network.

258. The combination of Lefebvre and Chua renders obvious claim 44.

259. Claim 44 is substantially the same as claim 21 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 44 for the same reasons discussed above for claim 21.

36. Claim 45: The method according to claim 32, wherein the first entity is a server device and the second entity is a client device, or wherein the first entity is a client device and the second entity is a server device.

260. The combination of Lefebvre and Chua renders obvious claim 45.

261. Claim 45 is substantially the same as claim 22 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 45 for the same reasons discussed above for claim 22.

37. Claim 46: The method according to claim 45, wherein the server device comprises a web server, and wherein the client device comprises a smartphone, a tablet computer, a personal computer, a laptop computer, or a wearable computing device.

262. The combination of Lefebvre and Chua renders obvious claim 46.

263. Claim 46 is substantially the same as claim 23 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 46 for the same reasons discussed above for claim 23.

38. Claim 47: The method according to claim 45, wherein the communication with the controller is based on, or uses, a standard protocol.

264. The combination of Lefebvre and Chua renders obvious claim 47.

265. Claim 47 is substantially the same as claim 24 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 47 for the same reasons discussed above for claim 24.

39. Claim 48: The method according to claim 47, wherein the standard protocol is according to, based on, or compatible with, an OpenFlow protocol version 1.3.3 or 1.4.0.

266. The combination of Lefebvre and Chua renders obvious claim 48.

267. Claim 48 is substantially the same as claim 25 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 48 for the same reasons discussed above for claim 25.

40. Claim 49: The method according to claim 48, wherein the instruction comprises a Type-Length-Value (TLV) structure.

268. The combination of Lefebvre and Chua renders obvious claim 49.

269. Claim 49 is substantially the same as claim 26 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 49 for the same reasons discussed above for claim 26.

41. Claim 50: The method according to claim 32, wherein the network node comprises a router, a switch, or a bridge.

270. The combination of Lefebvre and Chua renders obvious claim 50.

271. Claim 50 is substantially the same as claim 27 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 50 for the same reasons discussed above for claim 27.

42. Claim 51: The method according to claim 32, wherein the packet network is an Internet Protocol (IP) network, and the packet is an IP packet.

272. The combination of Lefebvre and Chua renders obvious claim 51.

273. Claim 51 is substantially the same as claim 28 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 51 for the same reasons discussed above for claim 28.

43. Claim 52: The method according to claim 51, wherein the packet network is a Transmission Control Protocol (TCP) network, and the packet is an TCP packet.

274. The combination of Lefebvre and Chua renders obvious claim 52.

275. Claim 52 is substantially the same as claim 29 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 52 for the same reasons discussed above for claim 29.

44. Claim 53: The method according to claim 32, further comprising: receiving, from the first entity over the packet network, one or more additional packets; checking, if any one of the one or more additional packets satisfies the criterion; responsive to an additional packet not satisfying the criterion, sending over the packet network, the additional packet to the second entity; and responsive to the additional packet satisfying the criterion, sending the additional packet over the packet network, in response to the instruction.

276. The combination of Lefebvre and Chua renders obvious claim 53.

277. Claim 53 is substantially the same as claim 30 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 53 for the same reasons discussed above for claim 30.

45. Claim 54: The method according to claim 32, wherein the packet network is a Software Defined Network (SDN), the packet is routed as part of a data plane and the communication with the controller serves as a control plane.

278. The combination of Lefebvre and Chua renders obvious claim 54.

279. Claim 54 is substantially the same as claim 31 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 54 for the same reasons discussed above for claim 31.

D. Ground 2: Claims 7, 8, 37, and 38 are rendered obvious by Lefebvre in view of Chua and Rash

280. Based on the following analysis, I conclude that a POSITA at the relevant time (April 22, 2014) would have understood the limitations of claims 7, 8, 37, and 38 were expressly disclosed, taught, or suggested by Lefebvre in combination with Chua and Rash. In my opinion, claims 7, 8, 37, and 38 would have been obvious to a POSITA in view of the prior art.

281. As I discussed above in Section VI, well before 2014, both SDN and DPI were well-known and ubiquitous. For example, both Lefebvre and Chua discuss SDN and DPI. *See, e.g.*, Lefebvre at 1:21-25, 1:34-38; Chua at 10:48-52, 31:48-59. Lefebvre and Chua both disclose how DPI often executes in dedicated service devices. *See, e.g.*, Lefebvre at 1:21-25, 1:34-38; Chua at 31:54-59 (describing DPI service devices). Chua specifically discloses the SDN controller performing DPI as well. *See* Chua at 31:48-54.

282. Rash discloses how network devices transmit portions of the packet to destinations other than the original intended destination. *See, e.g.*, Rash at 7:51-59, 9:3-12, 25:30-55, 26:11-35, 27:31-43, 29:58-62, 35:66-36:2. Rash discloses its dynamic mirroring functionality helps minimize the data mirrored to identification

appliances or other infrastructure devices configured to carry out the application identification function. See Rash at 12:59-13:8, 34:43-51. And Rash discloses the applicability of its dynamic traffic mirroring function for intrusion detection systems and network access control, among other applications. Rash at 10:29-56.

1. Motivation to Combine Lefebvre, Chua, and Rash

283. It is my opinion that a POSITA would have been motivated and found it obvious to modify Lefebvre with Rash's teachings. Lefebvre discloses techniques for an SDN to steer traffic through inline services. Lefebvre at 1:13-21, 2:39-47. Lefebvre discloses how operators can define the traffic classes and service chains for those classes for processing traffic flows on a per packet basis. Lefebvre at 4:41-43. Lefebvre discloses these operator instructions are programmed into the switches as rules so that the network traffic passes through the ordered chain of services as desired. Lefebvre at 4:41-47.

284. Lefebvre identifies several types of services that could form part of the service chain, including DPI. Lefebvre at 1:28-38, 4:48-54. Regarding DPI, Lefebvre discloses "[t]hese services are usually packaged and sold as dedicated appliance (either physical or virtual) and are often expensive." Lefebvre at 1:25-27, 1:34-38. One reason Lefebvre offers for implementing traffic steering is to direct traffic away from expensive services like DPI, reducing the need to invest in new service appliances. Lefebvre at 1:32-38. Lefebvre therefore controls the usage of

DPI services by routing network traffic through the service only as appropriate, where the services are separate from the controller.

285. Like Lefebvre, Rash discloses packet inspection systems. Rash at 7:31-34. Rash discloses a packet mirroring function that “provides the capability to select options based on a plurality of criteria to mirror any portion or all of the frames of packets received on the network.” Rash at 9:1-12, 27:31-43. Rash discloses that a network control manager controls the mirroring function. Rash at 9:12-15, 29:46-30:17. Rash’s packet mirroring device may be part of the network infrastructure. Rash at 25:30-55. Rash discloses the purpose of the mirroring may include application identification, security, or even ease of use, and the destination may exist either logically or physically. Rash at 26:11-35. Rash discloses how the mirrored traffic may have a different destination based on certain criteria. Rash at 35:66-36:2. And Rash discloses its dynamic mirroring functionality helps minimize the data mirrored to identification appliances or other infrastructure devices configured to carry out the application identification function. Rash at 12:59-13:8, 34:43-51.

286. A POSITA would have been motivated to modify Lefebvre with Rash to minimize the amount of network capacity used to examine packets, which would help reduce network costs and improve overall efficiency. A POSITA would have been motivated and found it obvious to modify Lefebvre with Rash’s teachings because both describe configurable networks, and both describe packet inspection

as one type of service available in these networks. Lefebvre at 1:28-38; Rash at 9:12-15, 25:30-55, 26:11-35, 29:46-30:17. Lefebvre and Rash are therefore in the same field of endeavor and contain overlapping disclosures with similar purposes.

287. Modifying Lefebvre in view of Rash’s teachings would have been obvious to a POSITA. Lefebvre has three different levels of policies which have different levels of granularity. Lefebvre at 6:32-48. Similarly, Rash explains that the network control engine may use packet fields including address, protocol, length or byte count, and other fields when making its mirroring determinations. Rash at 29:53-58.

288. Although Lefebvre mentions DPI as one type of known service, it considers packets in their entirety and similarly forwards packets in their entirety. *See, e.g.*, Lefebvre at 6:5-31, 1:28-38 (discussing DPI), 7:42-8:65. Rash provides specific details as to how entire packets or just portions of packets are mirrored. Rash at 9:1-12, 27:31-43. Rash discloses this targeted approach to mirroring minimizes the data the application identification function must consider. Rash at 12:59-13:8, 34:43-51. A POSITA would therefore look to Rash’s detailed teachings regarding mirroring of packets and portions of packets and apply them to Lefebvre.

289. A POSITA would have been motivated to modify Lefebvre with Rash’s teachings for multiple reasons. Lefebvre discloses that services including DPI “are usually packaged and sold as dedicated appliances (either physical or virtual) and

are often expensive.” Lefebvre at 1:25-27, 1:34-38. Rash similarly acknowledges the complexity and expense associated with deploying application identification functions in the network. Rash at 30:18-27. Rash explains its dynamic mirroring function leverages existing capabilities in network devices, thereby minimizing additional costs. Rash at 30:29-44, 34:37-47. Rash also discloses this targeted approach to mirroring minimizes the data the application identification function must consider. Rash at 12:59-13:8, 34:43-51. By implementing Rash’s mirroring of a portion of a packet instead of the entirety of a packet, a POSITA would recognize the network would experience a corresponding reduction in the amount of network capacity utilized to examine the packets, thereby reducing network costs and improving overall efficiency.

290. Implementing Rash’s teachings in Lefebvre’s controller would have been well within the skill of a POSITA. Lefebvre already redirects entire packets to the appropriate service. Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions). Similarly, Rash discloses mirroring packets to the network infrastructure that analyzes the mirrored traffic. *See, e.g.*, Rash at 7:51-57, 27:15-30 (disclosing the “mirrored traffic destination” includes any device “arranged to receive and either transfer or analyze the mirrored frames”). Modifying Lefebvre to forward only a portion of the packet as Rash teaches would have been well within the skill of a POSITA, as Rash confirms.

291. A POSITA would have had a reasonable expectation of success in applying Rash’s teachings to Lefebvre. Lefebvre already redirects the entirety of packets, so a POSITA would need to modify Lefebvre to consider a portion of a packet. *See* Lefebvre at 8:49-65, Table 1, Table 2 (depicting OpenFlow switch table actions). Rash’s technique allow for “any granularity of the frame of the network traffic” and Rash itself explains that “[o]ne ordinarily skilled in the art will recognize and appreciate that all or any portion of network traffic, such as all or any available portion of a frame, a packet, or any other protocol data unit, at one or more network protocol layers may be mirrored in practicing the operations of the present invention described herein.” Rash at 27:39-43; *see also* Rash at 27:44-53. Rash’s technique therefore relies on nothing more than a POSITA’s knowledge of how to take any portion of a protocol data unit. Because Rash confirms its teachings of mirroring portions of a protocol data unit are within a POSITA’s knowledge and ordinary skill, it is my opinion that a POSITA would have had a reasonable expectation of success in applying Rash’s teachings to Lefebvre. And similarly, it is my opinion that implementing this modification would have been simple and straightforward for a POSITA, requiring nothing more than a POSITA’s routine skill.

2. Claim 7: The method according to claim 5, further comprising responsive to the packet satisfying the criterion and to the instruction, sending a portion of the packet, by the network node, to the controller.

292. The combination of Lefebvre and Chua renders obvious the method of claim 5 set forth above. The combination of Lefebvre, Chua, and Rash renders obvious claim 7.

293. As discussed for claim element 1[f], the combination of Lefebvre and Chua renders obvious the claimed “responsive to the packet satisfying the criterion and to the instruction” aspect of claim 7. And Lefebvre and Chua acknowledge the different aspects of a packet, including the header field. Lefebvre at 15:54-63 (discussing considering the header fields of a packet), 16:67-17:2 (same); Chua at 25:57-61. But Lefebvre and Chua do not disclose sending a portion of the packet to the controller.

294. Rash discloses a packet inspection system that transmits portions of the packet to a destination other than the intended destination. Rash at 7:51-59, 9:3-12, 25:30-55, 26:11-35, 27:31-43, 29:58-62, 35:66-36:2. Rash discloses a network control manager, controlling the mirroring function, which provides the ability to select options “to mirror any portion or all of the frames of packets.” Rash at 9:1-15, 27:31-43, 29:7-12, 29:46-30:17.

295. As discussed in Section VII.D.1, a POSITA would have been motivated and found it obvious to apply Rash’s teachings to Lefebvre’s network. And Rash

discloses that this mirroring (the claimed instruction) sends the portion of packets to “the application identification engine” of the network. *See, e.g.*, Rash at 7:51-57, 27:15-30 (disclosing the “mirrored traffic destination” includes any device “arranged to receive and either transfer or analyze the mirrored frames”). So, Lefebvre’s network, as modified by Rash, would mirror portions of packets to the controller which, as modified by Chua, would execute DPI.

296. The combination of Lefebvre, Chua, and Rash therefore renders obvious dependent claim 7.

3. Claim 8: The method according to claim 7, wherein the portion of the packet consists of multiple consecutive bytes, and wherein the instruction comprises identification of the consecutive bytes in the packet.

297. The combination of Lefebvre, Chua, and Rash renders obvious dependent claim 8.

298. As discussed for claim 7, Lefebvre, Chua, and Rash teach sending a portion of the packet to the controller. Further, Rash discloses that, “based on a plurality of criteria,” its mirroring function can “mirror ... the first L bytes.” Rash at 9:3-12; *see also* Rash at 29:7-12, 29:46-62. A POSITA would have understood this to mean that Rash teaches mirroring multiple consecutive bytes (e.g., “the first L bytes”), and that the mirroring (the claimed instruction) identifies the consecutive bytes for mirroring.

299. The combination of Lefebvre, Chua, and Rash therefore renders obvious dependent claim 8.

- 4. Claim 37: The method according to claim 36, further comprising responsive to the packet satisfying the criterion and to the instruction, sending a portion of the packet to the controller.**

300. The combination of Lefebvre, Chua, and Rash renders obvious claim 37.

301. Claim 37 is substantially the same as claim 7 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 37 for the same reasons discussed above for claim 7.

- 5. Claim 38: The method according to claim 37, wherein the portion of the packet consists of multiple consecutive bytes, and wherein the instruction comprises identification of the consecutive bytes in the packet.**

302. The combination of Lefebvre, Chua, and Rash renders obvious claim 38.

303. Claim 38 is substantially the same as claim 8 addressed above. Thus, the combination of Lefebvre and Chua renders obvious claim 38 for the same reasons discussed above for claim 8.

E. Ground 3: Claims 16-20 and 39-43 are rendered obvious by Lefebvre in view of Chua and RFC 793

304. Based on the following analysis, I conclude that a POSITA at the relevant time (April 22, 2014) would have understood the limitations of Claims 16-

20 were expressly disclosed, taught, or suggested by Lefebvre in combination with Chua and RFC 793. In my opinion, claims 16-20 and 39-43 would have been obvious to a POSITA in view of the prior art.

1. Motivation to Combine RFC 793 with Lefebvre and Chua

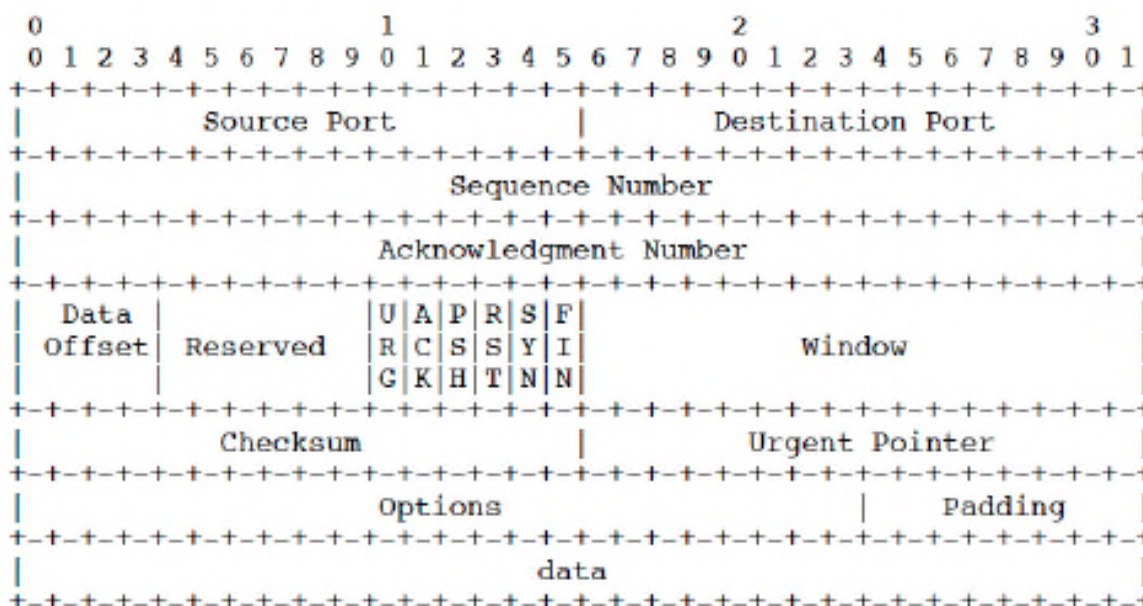
305. As explained above, RFC 793 defines the well-known and widely used Transmission Control Protocol (TCP). Both Lefebvre and Chua expressly contemplate use of their respective systems with TCP. *See, e.g.*, Lefebvre at 6:38-41 (describing policies that “are defined in terms of an IP address block and/or a User Datagram Protocol (UDP)/Transmission Control Protocol (TCP) port”), 7:60-67 (describing use of TCP/UDP source and destination ports); Chua at 18:12-15 (describing determining appropriate type of flow troubleshooting that includes the appropriate IP ranges to watch on, and the TCP/UDP services that the flowchain is meant to service), 23:52-56 (describing scenarios involving TCP client). RFC 793 discloses details of TCP that would have been familiar to a POSITA. In the context of systems such as Lefebvre and Chua that utilize TCP, a POSITA would have been motivated to look to RFC 793 for implementation details in order to ensure compliance with the Transmission Control Protocol. I provide additional explanation regarding the rationale and motivation for combining RFC 793 with Lefebvre and Chua with respect to the subject matter of claims 16-20 and 39-43 in the analysis that follows.

2. **Claim 16: The method according to claim 1, wherein the packet comprises distinct header and payload fields, the header comprises one or more flag bits, and wherein the packet-applicable criterion is that one or more of the flag bits is set.**

306. The combination of Lefebvre and Chua renders obvious the method according to claim 1 as discussed above in Ground 1. The combination of Lefebvre and Chua in further view of RFC 793 renders obvious dependent claim 16.

307. A POSITA would have understood that a packet comprises distinct header and payload fields. For example, a POSITA would have understood that Transmission Control Protocol (TCP) packets include separate and distinct header and payload fields. And a POSITA would have further understood that standard TCP packets include flag bits providing additional information related to the state of the connection. RFC 793, published September 1981, defines TCP. *See* EX1015, RFC 793 (available at <https://www.rfc-editor.org/rfc/pdf/rfc793.txt.pdf>). I have reproduced below Figure 3 of RFC 793 which depicts the TCP header format. RFC 793 at 15.

TCP Header Format



TCP Header Format

Note that one tick mark represents one bit position.

Figure 3.

308. Each TCP header includes source and destination port fields, a sequence number field, along with acknowledgement number, control bits, window, checksum, urgent pointer, and options fields. RFC 793 at 15-18. And RFC 793 defines optional features that could exist in the options field including no-operation and maximum segment size. RFC 793 at 18-19. Over time, other options including selective acknowledgements (SACK) and timestamps have utilized the TCP header options fields.

309. Lefebvre discloses using policies that consider other standard TCP header fields when classifying traffic, including source and destination addresses,

source and destination ports, and protocol fields. *See, e.g.*, Lefebvre at 15:55-60 (describing “assigning an ordered list of services to be applied to the packet in accordance with at least one header field of the packet” where the field may include “a source address, a destination address, a source port, a destination port or a protocol”); *see also* Lefebvre at 2:44-64, 3:33-45, 16:1-3 (“[t]he default service set can be optionally modified in accordance with at least one header field of the received packet”), 16:67-17:2 (same), 16:58-61 (“[t]he processor 706 can associate the received packet with the service set based on the determined direction and a header field of the packet”), claims 4, 5, 8, 9, 18, 21. Each TCP packet header includes the standard fields defined by RFC 793 such as source and destination ports and addresses, which Lefebvre already considers, and flag bits, which Lefebvre does not indicate it considers when classifying traffic. Chua similarly confirms the various header fields included with TCP packets including source and destination ports. Chua at 26:30-36.

310. Both Lefebvre and Chua discuss several various header fields but do not specifically identify the flag bits of TCP packets. But, as I explained and RFC 793 confirms, flag bits are part of the TCP standard. It is therefore my opinion that these would have been obvious to a POSITA to modify Lefebvre to consider the flag bits. A POSITA would have been motivated to modify Lefebvre to consider the status of the flag bits which provide additional information regarding the

connection's state and are part of the TCP standard. Modifying Lefebvre to consider the status of these standard additional fields of the TCP header would therefore allow Lefebvre's traffic steering to consider connection state when determining which service chain the packets should traverse, and each TCP packet includes these flag bits. Modifying Lefebvre to consider these flag bits would have been well within the skill of a POSITA. Lefebvre already considers other standard aspects of TCP packet headers, so modifying Lefebvre to consider the flag bits in addition to other aspects of the header field would have been well within the ordinary skill of a POSITA. *See, e.g.*, Lefebvre at 15:55-60 (describing "assigning an ordered list of services to be applied to the packet in accordance with at least one header field of the packet" where the field may include "a source address, a destination address, a source port, a destination port or a protocol"); *see also* Lefebvre at 2:44-64, 3:33-45, 16:1-3 ("[t]he default service set can be optionally modified in accordance with at least one header field of the received packet"), 16:67-17:2 (same), 16:58-61 ("[t]he processor 706 can associate the received packet with the service set based on the determined direction and a header field of the packet"), claims 4, 5, 8, 9, 18, 21. Indeed, Chua discloses how the controller programs network devices to perform actions including forwarding based on header data such as source and destination ports. Chua at 26:30-36.

311. The combination of Lefebvre and Chua in further view of RFC 793 therefore renders obvious dependent claim 16.

3. **Claim 17: The method according to claim 16, wherein the packet is an Transmission Control Protocol (TCP) packet, and wherein the one or more flag bits comprises comprise a SYN flag bit, an ACK flag bit, a FIN flag bit, a RST flag bit, or any combination thereof.**

312. The combination of Lefebvre and Chua in further view of RFC 793 renders obvious dependent claim 17.

313. As discussed for claim 16, a POSITA would have found it obvious to modify Lefebvre to consider TCP packet flag bits. As RFC 793 confirms, a POSITA would have also understood that TCP packet flag bits include the SYN, ACK, FIN, and RST flag bits, among others. These are some of the standard flag bits defined as part of the TCP standard. RFC 793 at 16 (describing the defined control bits including SYN, ACK, FIN, and RST).

314. The combination of Lefebvre and Chua in further view of RFC 793 therefore renders obvious dependent claim 17.

4. **Claim 18: The method according to claim 1, wherein the packet comprises distinct header and payload fields, the header comprises at least the first and second entities addresses in the packet network, and wherein the packet-applicable criterion is that the first entity address, the second entity address, or both match a predetermined address or addresses.**

315. The combination of Lefebvre and Chua renders obvious the method according to claim 1 as discussed above in Ground 1. The combination of Lefebvre and Chua in further view of RFC 793 renders obvious dependent claim 18.

316. A POSITA would have understood that IP packets include separate and distinct header and payload fields. *See* RFC 793 at 15 (describing “Internet Protocol header”); *see also* EX1008, 1 (“A packet is composed with header and payload[.]”). And a POSITA would have understood that IP packets include source and destination addresses. *See* RFC 793 at 15 (“The Internet Protocol Header carries several information fields, including the source and destination host addresses.”).

317. Confirming this, Lefebvre discloses associating a service set based on the direction of the packet and the header fields of packets including the “source address, a destination address, a source port, a destination port and a protocol.” Lefebvre at 2:47-52, 7:59-67, 8:4-30. The source and destination addresses Lefebvre discloses matching against in the header fields are the claimed first and second entities addresses in the packet network, and the addresses Lefebvre uses to identify the matching packets are the claimed predetermined addresses.

318. The combination of Lefebvre and Chua in further view of RFC 793 therefore renders obvious dependent claim 18.

5. Claim 19: The method according to claim 18, wherein the addresses are Internet Protocol (IP) addresses.

319. The combination of Lefebvre and Chua in further view of RFC 793 renders obvious dependent claim 19.

320. As discussed for claim 18, IP packets include source and destination addresses. A POSITA would have understood these addresses are IP addresses.

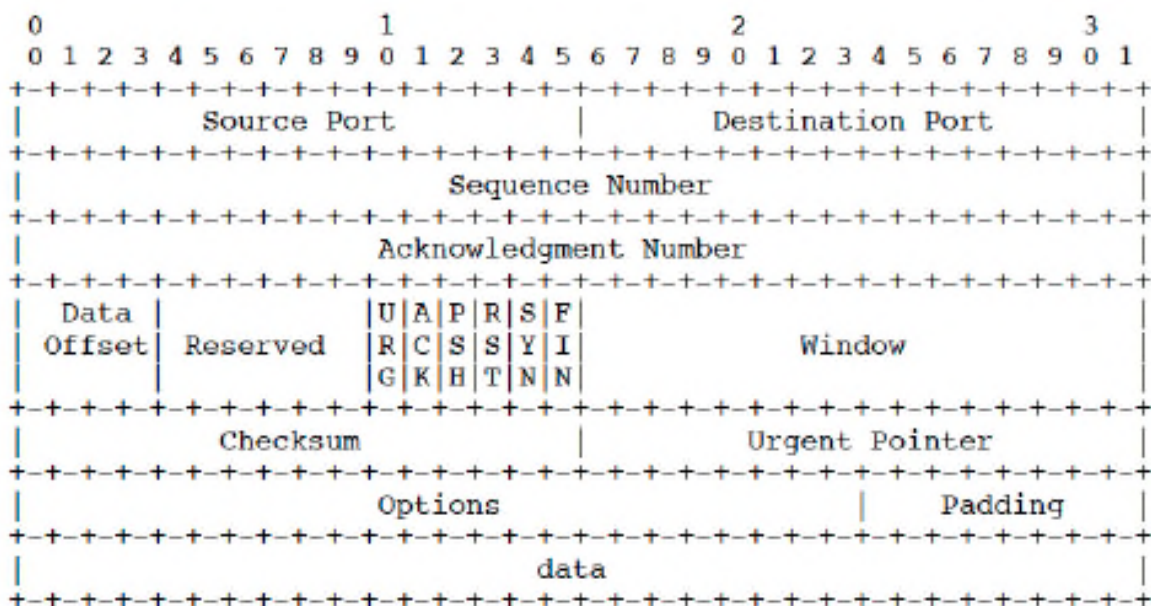
321. The combination of Lefebvre and Chua in further view of RFC 793 therefore renders obvious dependent claim 19.

6. Claim 20: The method according to claim 1, wherein the packet is an Transmission Control Protocol (TCP) packet that comprises source and destination TCP ports, a TCP sequence number, and a TCP sequence mask fields, and wherein the packet-applicable criterion is that the source TCP port, the destination TCP port, the TCP sequence number, the TCP sequence mask, or any combination thereof, matches a predetermined value or values.

322. The combination of Lefebvre and Chua renders obvious the method according to claim 1 as discussed above in Ground 1. The combination of Lefebvre and Chua in further view of RFC 793 renders obvious dependent claim 20.

323. As discussed, RFC 793, published September 1981, defines TCP. *See* RFC 793. I have reproduced below Figure 3 of RFC 793 which depicts the TCP header format.

TCP Header Format



TCP Header Format

Note that one tick mark represents one bit position.

Figure 3.

RFC 793 at 15.

324. Each TCP header includes source and destination port fields, a sequence number field, along with acknowledgement number, control bits, window, checksum, urgent pointer, and options fields. RFC 793 at 15-19. And RFC 793 defines optional features that could exist in the options field including no-operation and maximum segment size. RFC 793 at 18-19. I note that nothing in RFC 793 constitutes a “TCP sequence mask” field, as claim 20 recites. And nothing in the ’111 Patent explains what makes up the “TCP sequence mask” field. Rather, the

'111 Patent explains how to compute the TCP sequence mask. '111 Patent at 4:58-60, 6:41-7:40, 9:56-61.

325. I have been asked to assume that the claims are not indefinite. Regardless of what TCP header field corresponds to “TCP sequence mask,” the combination of Lefebvre and Chua renders claim 20 obvious. This is because a POSITA would have understood that TCP packets (more typically referred to as TCP segments) include each of the fields required by RFC 793, including source and destination ports, and TCP sequence numbers. Lefebvre discloses using the source and destination port and address fields along with the protocol fields, but does not specifically identify the TCP sequence number. Lefebvre at 15:55-60 (describing “assigning an ordered list of services to be applied to the packet in accordance with at least one header field of the packet” where the field may include “a source address, a destination address, a source port, a destination port or a protocol”).

326. Regardless, because the sequence number is part of the TCP standard, defined by RFC 793, as are the fields Lefebvre already considers, it is my opinion that it would have been obvious to a POSITA to modify Lefebvre to consider the source and destination addresses, the TCP sequence number, and any other fields necessary to constitute the claimed “TCP sequence mask” field.

327. A POSITA would have been motivated to modify Lefebvre to consider these additional standard fields which provide additional information regarding the

session including what portion of the data stream the TCP segment constitutes. Lefebvre's traffic steering already considers other standard TCP header fields when classifying traffic, including source and destination addresses, source and destination ports, and protocol fields. See Lefebvre at 15:55-60 (describing "assigning an ordered list of services to be applied to the packet in accordance with at least one header field of the packet" where the field may include "a source address, a destination address, a source port, a destination port or a protocol"); *see also* Lefebvre at 2:44-64, 3:33-45, 16:1-3 ("[t]he default service set can be optionally modified in accordance with at least one header field of the received packet"), 16:67-17:2 (same), 16:58-61 ("[t]he processor 706 can associate the received packet with the service set based on the determined direction and a header field of the packet"), claims 4, 5, 8, 9, 18, 21. Each TCP packet header includes the standard fields defined by RFC 793 such as source and destination ports and addresses, which Lefebvre already considers, and sequence numbers, which Lefebvre does not. Modifying Lefebvre to consider additional standard fields would allow Lefebvre's traffic steering to consider the details provided by these additional standard fields when classifying traffic and determining which service chain the packets should traverse. Modifying Lefebvre to consider these additional standard fields would have been well within the skill of a POSITA. Lefebvre already considers other standard aspects of TCP headers, so parsing and considering additional standard fields would have

been well within the ordinary skill of a POSITA. Chua provides evidence of this when disclosing how the controller programs network devices to perform actions including forwarding based on standard TCP header data such as source and destination ports. *See, e.g.*, Chua at 16:27-30.

328. The combination of Lefebvre and Chua therefore renders obvious dependent claim 20.

7. **Claim 39: The method according to claim 32, wherein the packet comprises distinct header and payload fields, the header comprises one or more flag bits, and wherein the packet-applicable criterion is that one or more of the flag bits is set.**

329. The combination of Lefebvre and Chua renders obvious the method according to claim 32 as discussed above in Ground 1. The combination of Lefebvre and Chua in further view of RFC 793 renders obvious dependent claim 39.

330. Claim 39 is substantially the same as claim 16 addressed above. Thus, the combination of Lefebvre and Chua in further view of RFC 793 renders obvious claim 39 for the same reasons discussed above for claim 16.

8. **Claim 40: The method according to claim 39, wherein the packet is an Transmission Control Protocol (TCP) packet, and wherein the one or more flag bits comprises comprise a SYN flag bit, an ACK flag bit, a FIN flag bit, a RST flag bit, or any combination thereof.**

331. The combination of Lefebvre and Chua in further view of RFC 793 renders obvious claim 40.

332. Claim 40 is substantially the same as claim 17 addressed above. Thus, the combination of Lefebvre and Chua in further view of RFC 793 renders obvious claim 40 for the same reasons discussed above for claim 17.

- 9. Claim 41: The method according to claim 32, wherein the packet comprises distinct header and payload fields, the header comprises at least the first and second entities addresses in the packet network, and wherein the packet-applicable criterion is that the first entity address, the second entity address, or both match a predetermined address or addresses.**

333. The combination of Lefebvre and Chua renders obvious the method according to claim 32 as discussed above in Ground 1. The combination of Lefebvre and Chua in further view of RFC 793 renders obvious dependent claim 41.

334. Claim 41 is substantially the same as claim 18 addressed above. Thus, the combination of Lefebvre and Chua in further view of RFC 793 renders obvious claim 41 for the same reasons discussed above for claim 18.

- 10. Claim 42: The method according to claim 41, wherein the addresses are Internet Protocol (IP) addresses.**

335. The combination of Lefebvre and Chua in further view of RFC 793 renders obvious claim 42.

336. Claim 42 is substantially the same as claim 19 addressed above. Thus, the combination of Lefebvre and Chua in further view of RFC 793 renders obvious claim 42 for the same reasons discussed above for claim 19.

11. **Claim 43: The method according to claim 32, wherein the packet is an Transmission Control Protocol (TCP) packet that comprises source and destination TCP ports, a TCP sequence number, and a TCP sequence mask fields, and wherein the packet-applicable criterion is that the source TCP port, the destination TCP port, the TCP sequence number, the TCP sequence mask, or any combination thereof, matches a predetermined value or values.**

337. The combination of Lefebvre and Chua renders obvious the method according to claim 32 as discussed above in Ground 1. The combination of Lefebvre and Chua in further view of RFC 793 renders obvious dependent claim 43.

338. Claim 43 is substantially the same as claim 20 addressed above. Thus, the combination of Lefebvre and Chua in further view of RFC 793 renders obvious claim 43 for the same reasons discussed above for claim 20.

VIII. SECONDARY CONSIDERATIONS

339. During prosecution of the '111 Patent, the applicant did not identify any evidence of secondary considerations of non-obviousness tied to the claimed invention of the '111 Patent. I understand from counsel for Petitioner that Patent Owner in the co-pending district court litigation has not yet identified any evidence with respect to secondary considerations of non-obviousness.

340. Accordingly, there is no objective evidence of non-obviousness that might warrant a finding that claims 1-54 are patentable. To the extent the Patent Owner at a later date cites or provides any other evidence regarding secondary

considerations, including any expert opinions, I reserve the right to supplement my analysis and opinions to address it.

IX. CONCLUSION

341. For at least the above-described reasons, in my opinion claims 1-54 of the '111 Patent would have been obvious to a POSITA based on the prior art references that I have cited and analyzed above.

342. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

343. I reserve the right to supplement my opinions in the future to respond to any arguments raised by Patent Owner and to consider any new information that becomes available to me.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further 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.

Executed this 1st day of August, 2024, in St. Louis, Missouri.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Paul Min", written over a horizontal line.

Paul Min, Ph.D.

APPENDIX A

Paul S. Min, Ph.D.
Washington University in Saint Louis
(Webpage : <https://engineering.wustl.edu/faculty/Paul-Min.html>)

psm@wustl.edu
+1 (314) 853-6200 (phone)

Campus Box 1223
Academy Building Room 218A
St. Louis, MO 63130

Education

<u>Year</u>	<u>College or University</u>	<u>Degree</u>
1987	The University of Michigan	Ph.D. in Electrical Engineering
1984	The University of Michigan	M.S. in Electrical Engineering
1982	The University of Michigan	B.S. in Electrical Engineering

Professional Experience

From: 1990
To: Present
Organization: Washington University, St. Louis

Summary:

2015 - Senior Professor - Department of Electrical Systems Engineering

2011 – 2014 Chair – Undergraduate Curriculum, Department of Electrical and Systems Engineering

2000 – 2002 Chair – Graduate Curriculum, Department of Electrical and Systems Engineering

2002 - 2014 Associate Professor - Department of Electrical and Systems Engineering

1997 - 2008 On leave from full-time duty at Washington University – as Presidents of MinMax Technologies and Erlang Technology.)

1996 - 2002 Associate Professor - Department of Electrical Engineering

1996 Promoted with Tenure

1990 - 1996 Assistant Professor - Department of Electrical Engineering

- Teaching Experience
- “Transmission System and Multiplexing,” Washington University, ESE 571
 - “Electrical Laboratory I,” Washington University, EE 250.
 - “Communication Theory,” Washington University, ESE 471.
 - “Reliability and Quality Control,” Washington University, ESE 405/505
 - “Signaling and Control of Communications Networks,” Washington University, ESE 572.
 - “Introduction to Electronic Circuits,” Washington University, ESE232
 - “Queueing Systems and Discrete Stochastic Processes,” Washington University, EE 536 / CS 567.
 - “Digital Computer,” Washington University, EE 260M / CS 260.
 - “Data Networks,” Washington University, EE 530.
 - “Electrical Circuit Analysis,” Washington University, ESE 230.
 - “Computer/Communications System Analysis I,” Washington University, EE 557/ CS 557.
 - “Computer/Communications System Analysis II,” Washington University, EE558 / CS 558.
 - “Digital Systems Laboratory,” Washington University, EE 455 / CS 455.

From: 1999
To: 2008
Organization: Erlang Technology, Inc., St. Louis, Missouri
Title: Founder and President
Summary: Up to 70 employees, \$40M in total capital raised from 5 VCs and 3 Corporations
Received “Product of Year” Award from Analog Zone Magazine in 2004

From: 1997
To: 1999
Organization: MinMax Technologies, Inc., St. Louis, Missouri
Title: Founder and President
Summary: Fabless semiconductor company, designing high performance switching ASICs

From: September 1987
To: August 1990
Organization: Bellcore, New Jersey
Title: Member of Technical Staff
Summary: Member of New Network Architecture Development Group

From: 1983
To: 1987

Organization: Department of Electrical Engineering, The University of Michigan
Title: Graduate Instructor
Summary: Instructor for senior level Electrical Engineering Laboratory Class. Received a Best “Best Graduate Instructor Award” from the Department of Electrical Engineering

Professional Affiliations, Achievements & Awards

- Technical Program Committee, COMCAS 2021, Tel Aviv, November 2021.
- Technical Program Committee, COMCAS 2019, Tel Aviv, November 2019.
- Technical Program Committee, COMCAS 2017, Tel Aviv, November 2017.
- Technical Program Committee, COMCAS 2015, Tel Aviv, October 2015.
- Past-Chair, Saint Louis Section of the Institute of Electrical and Electronics Engineers (IEEE), 2015.
- Member of Executive Committee, Saint Louis Section of the IEEE, 2010-2015.
- Chair, Saint Louis Section of the IEEE, 2014.
- Technical Program Committee, COMCAS 2013, Tel Aviv, October 2013.
- Vice Chair, Saint Louis Section of the IEEE, 2013
- Treasurer, Saint Louis Section of the IEEE, 2012.
- The Best Paper Award at MOBILITY 2011, October 2011, Barcelona, Spain.
- Counselor, Student Chapter of the Year, the Institute of Electrical and Electronics Engineers, 2011.
- Award of Appreciation, Saint Louis Section of the Institute of Electrical and Electronics Engineers, 2011, for contribution to various activities of the Saint Louis Section the Institute of Electrical and Electronics Engineers.
- Secretary, Saint Louis Section of the IEEE, 2010.
- Counselor, Student Chapter of the Year, the Institute of Electrical and Electronics Engineers, 2010.
- Wall Street Journal Businessmen of Year, 2003.
- American Men and Women of Science, listed in 1997.
- Member, Eta Kappa Nu (Honor Society for Electrical Engineers), inducted in 1992
- Outstanding Achievement Award, Bellcore, 1990.
- 18th ISATA Award of Technical Excellence, the best paper award at ISATA 1988.
- Rockwell Fellow, Rockwell International, 1985, 1986.
- Outstanding Graduate Student Award, the University of Michigan, 1985.
- Outstanding Teaching Award, the University of Michigan, 1984, 1986.
- Member of Honor's College, the University of Michigan, 1979, 1980.

- Honor's Convocation, the University of Michigan, 1979.
- Outstanding Freshman Award, the University of Michigan, 1979.
- Woodhaven Rotary Club Scholarship, Woodhaven Rotary Club, 1978.
- Second Place Winner, the State of Michigan Mathematics Prize Competition, 1977.
- International Program Committee, *IASTED International Conference on Communications, Internet and Information Technology (CIIT 2005)*, Cambridge, Massachusetts from October 31-November 2, 2005.
- International Program Committee, *IASTED International Conference on Communications 2003*, Scottsdale, Arizona, 2003.
- International Program Committee, *Wireless and Optical Communications 2003*, Banff, Canada, 2003.
- International Program Committee, Session Chair, *Wireless and Optical Communications 2002*, Banff, Canada, 2002.
- Invited participant, *NSF Workshop on Enhancing International Cooperation in CS/CE Research and Education*, Portland, 1997.
- Session Chair, *the 1993 Conference on Information Sciences and Systems*, Baltimore, March 1997.
- Member, Board of Editors, *Journal of Network and Systems Management*, 1996-1998.
- Program Committee, *International Symposium on Integrated Network Management*, San Diego, 1997.
- Guest Editor, *Journal of Network and Systems Management, Special Issue on Routing in Broadband Networks*, December 1995 and June 1996.
- Invited participant, *ARPA Workshop on Survivability of Large Scale Systems*, Washington D.C., 1996.
- Special Event Organizer, *International Symposium on Integrated Network Management*, Santa Barbara, 1995.
- Organizing Committee, *International Symposium on Integrated Network Management*, Santa Barbara, 1995.
- Local Arrangements Chair, *IEEE Information Theory Workshop on Information Theory Multiple Access and Queueing*, St. Louis, 1995.
- Chair, *Communications Chapter, St. Louis Section of the IEEE*, 1995.
- Participant, *IEEE Information Theory Workshop on Information Theory, Multiple Access and Queueing*, St. Louis, 1995.
- Participant, *ARPA/AFOSR Non-Linear Optics and Communication Workshop*, Denver, 1994.
- Participant, *CNRI Giga Bit Network Workshop*, Washington D.C., 1993.
- Participant, *IFIP/IEEE International Workshop on Distributed Systems*, New Jersey, 1993.
- Program Committee, *International Conference on Computer Communications and Networks*, San Diego, 1992.
- Session Chair, *ISMM International Conference*, New Orleans, 1990.
- Senior Member, *IEEE*.

- Member, *IEEE Committee on Network Operations and Management*.
- Member, *IEEE Committee on Computer Communications*.
- Registered Specialist, *Hong Kong Research Grant Council*.
- Reviewer, *IEEE Transactions on Communications*.
- Reviewer, *IEEE Transactions on Networking*.
- Reviewer, *IEEE Journal on Selected Areas in Communications*.
- Reviewer, *Journal of Network and Systems Management*.
- Reviewer, *Telecommunication Systems*.
- Reviewer, *Computers and Electrical Engineering*.
- Reviewer, *ETRI Journal*.
- Reviewer, *IEEE Transactions on Automatic Control*.
- Reviewer, *IEEE Communications*.
- Book Reviewer, *Prentice Hall*.
- Book Reviewer, *Morgan Kaufmann Publishers, Inc.*
- Book Reviewer, *Irwin Publishing Co.*

University Activities:

- Undergraduate Studies Committee, School of Engineering and Applied Science (2012 – Present)
- Faculty Advisor for IEEE Student Chapter (2009 – Present)
- Ambassador for McDonnell International Scholar Academy (2007 – 2013)
- Web Development Committee (2006 – 2008)
- University Judicial Board (1998 - 2000)
- Resource Generation Committee (1994 - 1995)
- Top 20 Committee (1992 - 1995)
- Telecommunications Committee, Chair (1991 - 1997)
- Library Planning Committee (1991 - 1992)
- Computer Engineering Committee (1990 - 1996)
- Communications Curriculum Committee (1990 - 1992)
- Resources Committee (1990 - 1992)

Patents

<u>Patent No.</u>	<u>Date</u>	<u>Title</u>
10,623,323	04/14/20	Network Devices and a Method for Signature Pattern Detection
10,284,476	05/07/19	Hierarchical Pattern Matching Devices and Methods

7,110,411	09/19/06	Method of and Apparatus for WFQ Scheduling Using a Plurality of Scheduling Queues to Provide Fairness, High Scalability, and Low Computational Complexity
7,106,738	09/12/06	Method of and Apparatus for High Speed Packet Switching Using Train Packet Queuing and Providing High Scalability
6,859,455	02/22/05	Method of and Apparatus for Building and Using Multi-Dimensional Index Trees for Multi-Dimensional Data Objects
6,614,789	09/02/03	Method of and Apparatus for Matching Strings of Different Lengths
6,359,885	3/19/02	Multi-Channel Packet Switching Apparatus Having Traffic Flow Controlling and Checking Functions
6,128,292	10/03/00	Packet Switching Apparatus with Multi-Channel and Multi-Cast Switching Functions and Packet Switching System Using the Same
5,788,161	12/13/98	Network Designer for Communication Networks
5,526,352	06/11/95	Integrable Low Complexity Multi-Channel Switch
5,440,549	08/08/95	Nonblocking Multi-Channel Switching with Multicasting Capability

Publications

- Yu, Qixiang, Luo, Z., and Min, P.S., “Intrusion Detection in Wireless Sensor Networks for Destructive Intruders.” Proceedings of the APSIPA 2015 conference. December 16-19, 2015.
- Hung, C.P., and Min, P.S., “Simple Web Application Framework.” Submitted for publication in the IEEE Transactions on Cloud Computing.
- Luo, Z., and Min, P.S., “Parallel Implementation of Energy-Based Target Localization Methods in Wireless Sensor Networks.” Proceeding of the 2014 IEEE SOUTHEASTCON.
- Yu, Q., Luo, Z., and Min, P.S., “Intrusion Detection in Wireless Sensor Networks for Destructive Intruder.” Proceeding of 2014 International Conference on Smart Computing (SMARTCOMP 2014).
- Luo, Z., and Min, P.S., “Survey of Target Localization Methods in Wireless Sensor Networks,” 19th IEEE International Conference on Networks (ICON 2013), Singapore, December 11-13, 2013.
- Hung, C.P., and Min, P.S., “Deriving and Visualizing the Lower Bounds of Information Gain for Prefetch Systems,” 19th IEEE International Conference On Networks (ICON 2013), Singapore, December 11-13, 2013.
- Hung, C.P., and Min, P.S., “Access LUT without CAM - Improved Pearson Hashing for Collision Reduction,” 19th IEEE International Conference On Networks (ICON 2013), Singapore, December 11-13, 2013.
- Luo, Z and Min, P.S., “Target Localization in Wireless Sensor Networks for Industrial Control with Selected Sensors.” International Journal of Distributed Sensor Networks, Volume 2013 (2013), Article ID 304631.
- Hung, C.P., and Min, P.S. “Performance Evaluation of Distributed Mobile Application Virtualization Services,” International Journal on Advances in Internet Technology, Vol. 5, no. 3&4, 2012, pp. 65-83.

- Hung, C.P. and Min, P.S., “Performance evaluation of distributed application virtualization services using the UMTS mobility model,” *MOBILITY 2011 The First International Conference on Mobile Services, Resources, and Users*, 23-29 Oct. 2011.
- Hung, C.P. and Min, P.S., “Service Area Optimization For Application Virtualization Using UMTS Mobility Model,” *International Conference on Internet Computing*, pp. 128-134, Las Vegas, July 18-21, 2011.
- Hung, C.P. and Min, P.S., “Application Virtualization Using UMTS Mobility Model,” *ICOMP'11*, September, 2011.
- Hung, C.P. and Min, P.S., “Infrastructure Arrangement for Application Virtualization Service,” the 9th International Information and Telecommunication Technologies Symposium, Vol.1, pp. 78-85, Rio de Janeiro, December 2010.
- Hung, C.P. and Min, P.S., “Probabilistic Approach to Network-Based Virtual Computing,” the 9th International Information and Telecommunication Technologies Symposium, Vol.1, pp. 117-124, Rio de Janeiro, December 2010.
- Shiravi, A. and Min, P. S., “On the Latency Bound of Proportional Nested-DRR with Credit Adjusting,” *2007 Workshop on High Performance Switching and Routing HPSR 2007*, July 2007.
- Shiravi, A. and Min, P. S., “LOOFA-PB: A Modified LOOFA Scheduler for Variable-Length Packet Switching.” *2007 IEEE International Conference on Communications (ICC 2007)*, Glasgow, June 2007.
- Shiravi, A., Kim, Y. G., and Min, P. S., “Congestion Prediction of Self-Similar Network through Parameter Estimation,” *Proceedings of 2006 IEEE/IFIP Network Operations & Management Symposium*, April 2006, Vancouver.
- Shiravi, A., Kim, Y. G., and Min, P. S., “Traffic Dispatching Algorithm in Three-Stage Switch,” *Proceedings of 5th International Conference on Networking*, April 2006, Mauritius.
- Shiravi, A., Kim, Y. G., and Min, P. S., “Proportional Nested Deficit Round Robin with Credit Adjusting,” *Proceedings of 2nd Int’l Conf. on Quality of Service in Heterogeneous Wired/Wireless Networks (QShine 2005)*, Orlando, August 2005.
- Shiravi, A., Kim, Y. G., and Min, P. S., “Proportional Nested Deficit Round Robin: Improving the Latency of Packet Scheduler with an O(1) Complexity,” *Proceedings of International Workshop on Advanced Architectures and Algorithms for Internet Delivery and Applications (AAA-IDEA 2005)*, Orlando, June 2005
- Kim, Y. G., Shiravi, A., and Min, P. S., “Prediction-Based Routing through Least Cost Delay Constraint,” *Proceedings of IEEE IPDPS 2004*, Santa Fe, April 2004.
- Kim, Y. G. and Min, P. S., “On the Prediction of Average Queuing Delay with Self-Similar Traffic,” *Proceedings of IEEE GLOBECOM 2003*, San Francisco, December 2003.
- Hu, C., Saidi, H., Yan, P. Y., and Min, P.S., “A Protocol Independent Policier And Shaper Using Virtual Scheduling Algorithm,” *Proceedings of ICCAS 2002*.

- Hu, C., Saidi, H., and Min, P.S., “DB_WFQ: An Efficient Fair Queueing Using Binary Counter,” *Proceeding of Coins 2002*.
- Yoon, U. and Min, P.S., “Performance Analysis of Radio Link Control Mechanism in W-CDMA System”, IEEE VTC’01 Fall, October 2001, New Jersey
- Akl, B., Hegde, M.V., Naraghi-Pour, M., and Min, P.S., “Multi-Cell CDMA Network Design,” *IEEE Transaction on Vehicular Technology*, Volume 50, No. 3, pp. 711-722, May 2001.
- Yoon, U., Park, S., Min, P.S., “Performance Analysis of Multiple Rejects ARQ at RLC (Radio Link Control) for Packet Data Service in W-CDMA System,” *IEEE Globecom*, November 2000, San Francisco.
- Yoon, U., Park, S., Min, P.S., “Performance Analysis of Multiple Rejects ARQ for RLC (Radio Link Control) in the Third Generation Wireless Communication,” *WCNC*, September 2000, Chicago.
- Yoon, U., Park, S., Min, P.S., “Network Architecture and Wireless Data Service Protocol based on Mobile IP toward the Third Generation Wireless Communication,” *3G Wireless*, June 2000, San Francisco, pp. 211-215
- R.G. Akl, M.V. Hegde, M. Naraghi-Pour, P.S. Min, “Multi-Cell CDMA Network Design,” *IEEE International Conference on Communications*, June 2000.
- R.G. Akl, M.V. Hegde, M. Naraghi-Pour, P.S. Min, “CDMA Network Design to Meet Non-uniform User Demand,” *International Teletraffic Congress*, March 2000.
- R.G. Akl, M.V. Hegde, M. Naraghi-Pour, P.S. Min, “CDMA Network Design,” *IEEE Transactions on Vehicular Technology*.
- R.G. Akl, M.V. Hegde, M. Naraghi-Pour, P.S. Min, “Cell Placement in a CDMA Network,” *IEEE Wireless Communications and Networking Conference*, September 1999, Volume 2, pp. 903-907.
- R.G. Akl, M.V. Hegde, P.S. Min, “Effects of Call Arrival Rate and Mobility on Network Throughput in Multi-Cell CDMA,” *IEEE International Conference on Communications*, June 1999, Volume 3, pp. 1763-1767.
- Hegde, M.V., Schmid, O.A., Saidi, H., and Min, P.S., “Real-Time Adaptive Bandwidth Allocation for High-Speed ATM Switches,” accepted, *International Conference on Communications*, June 1999.
- Akl, B.G., Hegde, M.V., and Min, P.S., “Effects of Mobility on Network Throughput in Multicell CDMA Networks,” accepted, *International Conference on Communications*, June 1999.
- Akl, B.G., Hegde, M.V., Min, P.S., and Naraghi-Pour, M., “Flexible Allocation of Capacity in Multi-Cell CDMA Networks,” accepted, *Vehicular Technology Conference*, June 1999.
- R.G. Akl, M.V. Hegde, M. Naraghi-Pour, P.S. Min, “Flexible Allocation of Capacity in Multi-Cell CDMA Networks,” *IEEE Vehicular Technology Conference*, May 1999, Volume 2, pp. 1643-1647.

- Oh, M.S., and Min, P.S., "Reliability Analysis for One-Turn and Deflection Crossbar Architectures and Distributed Fault Recovery Scheme," *Proceedings of GLOBECOM 97*, Phoenix, November 1997.
- Kim, K.B., Yan, P.Y., Kim, K.S., Schmid, O., and Min, P.S., "A Growable ATM Switch with Embedded Multi-Channel Multicasting Property," *Proceedings of GLOBECOM 97*, pp. 222-226, Phoenix, November 1997.
- Kim, K.B., Yan, P.Y., Kim, K.S., Schmid, O., and Min, P.S., "MASCON: A Single IC Solution to ATM Multi-Channel Switching with Embedded Multicasting," *Proceedings of ISS 97*, pp. 451-458, Toronto, September 1997.
- Maunder, A.S., and Min, P.S., "Investigation of Rate Control in Routing Policies for B-ISDN Networks," *Proceedings of the 15th International Teletraffic Congress*, Washington D.C., June 1997.
- Yan, P.Y., Kim, K.B., Kim, K.S., and Min, P.S., "A Large Scale ATM Switch System Using Multi-Channel Switching Paradigm," *Proceedings of ATM Workshop*, Lisbon, Portugal, May 1997.
- Yan, P.Y., Kim, K.S., Min, P.S., and Hegde, M.V., "Multi-Channel Deflection Crossbar (MCDC): A VLSI Optimized Architecture for Multi-Channel ATM Switching," *Proceedings of IEEE INFOCOM 97*, Kobe, Japan, April 1997.
- Maunder, A., Rayes, A., and Min, P.S., "Analysis and Rate Controlling Link: Leaky Bucket with Finite Servers," *Proceedings of the 1997 Conference on Information Sciences and Systems*, Baltimore, March 1997.
- Shin, S.W., Min, P.S., and Kim, J.H., "Real Time Traffic Management System at Korean Mobile Telecom," *Proceedings of 19th Annual Pacific Telecommunications Conference*, pp. 113-121, Honolulu, Hawaii, January 1997.
- Min, P.S., Hegde, M.V., Chandra, A., and Maunder, A.S., "Analysis of Banyan Based Copy Networks with Internal Buffering," *Journal of High Speed Networks*, Volume 5, No. 3, pp. 259-275 November 1996.
- Vargas, C., Hegde, M.V., Naraghi-Pour, M., and Min, P.S., "Shadow Prices for Least Loaded Routing and Aggregated Least Busy Alternate Routing," *IEEE Transactions on Networking*, Volume 4, No. 5, pp. 796-807, October 1996.
- Shin, S.W., Kwon, S.M., and Min, P.S., "Capacity Analysis of CDMA with Nonuniform Cell Loading and Sizes," *Proceedings of the 34th Annual Allerton Conference*, October 1996.
- Hegde, M.V., Min, P.S., and Sohraby, K., "Note from Guest Editors," *Journal of Network and Systems Management*, Volume 4, No. 2, pp. 101-102, June 1996.
- Rayes, A. and Min, P.S., "Application of Shadow Price in Capacity Expansion of State Dependent Routing," *Journal of Network Systems Management*, Volume 4, No. 1, pp. 71-93, March 1996.
- Min, P.S., "PCS Revolution in the United States," *Electronics News*, No. 2277, January 22, 1996. Translated and published in Korean.

- Hegde, M.V., Min, P.S., and Sohraby, K., "Guest Editorial," *Journal of Network and Systems Management*, Volume 3, No. 4, pp. 347-349, December 1995.
- Min, P.S., Hegde, M.V., Saidi, H., and Chandra, A., "Nonblocking Copy Networks in Multi-Channel Switching," *IEEE Transactions on Networking*, Volume 3, No. 6, pp. 857-871, December 1995.
- Rayes, A. and Min, P.S., "Capacity Expansion of Least Busy Alternate Routing with Shadow Price," *Proceedings of GLOBECOM 95*, Singapore, November 1995.
- Min, P.S., Hegde, M.V., Chandra, A., and Maunder, A., "Throughput and Delay for Copy Networks with Internal Buffers," *Proceedings of the 33rd Annual Allerton Conference*, October 1995.
- Min, P.S., Hegde, M.V., Saidi, H., and Chandra, A., "Fanout Splitting in Nonblocking Copy Networks with Shared Buffering," *Proceedings of the 33rd Annual Allerton Conference*, October 1995.
- Min, P.S., Hegde, M.V., and Rayes, A., "Estimation of Exogenous Traffic Based on Link Measurements in Circuit-Switched Networks," *IEEE Transactions on Communications*, Volume 43, No. 8, pp. 2381-2390, August 1995.
- Maunder, A., Rayes, A., and Min, P.S., "Analysis of Routing Policies in Broadband Networks." Invited paper. *Canadian Journal of Electrical and Computer Engineering*, Special Issue on Planning and Designing of Broadband Networks, Volume 20, No. 3, pp. 125-136, July 1995.
- Min, P.S., Hegde, M.V., Saidi, H., and Chandra, A., "Architecture and Performance of Nonblocking Copy Networks with Multi-Channel Switching," *Proceedings of APCC 95*, pp. 531-535, Osaka, Japan, June 1995.
- Saidi, H., Min, P.S., and Hegde, M.V., "A New Structural Property of Statistical Data Fork," *IEEE Transactions on Networking*, Volume 3, No. 3, pp. 289-298, June 1995.
- Min, P.S., Saidi, H., and Hegde, M.V., "A Nonblocking Architecture for Broadband Multi-Channel Switching," *IEEE Transactions on Networking*, Volume 3, No. 2, pp. 181-198, April 1995.
- Min, P.S., Hegde, M.V., Saidi, H., and Chandra, A., "Multi-Channel Copy Networks: Architecture, Performance Model, Fairness, and Cell Sequencing," *Proceedings of IEEE INFOCOM 95*, pp. 931-938, Boston, April 1995.
- Min, P.S., Hegde, M.V., and Chandra, A., "Analysis of Packet Movements in Internally Buffered Copy Networks," *Third ORSA Telecommunications Conference*, p. 141, Boca Raton, Florida, March 1995.
- Maunder, A. and Min, P.S., "Routing for Multi-Rate Traffic with Multiple Qualities of Service," *Proceedings of the Third International Conference on Computer Communications and Networks*, pp. 104-108, San Francisco, September 1994.
- Saidi, H. and Min, P.S., "Performance Benefits of Multi-Channel Switching," *Proceedings of the 32nd Annual Allerton Conference*, pp. 583-592, September 1994.
- Min, P.S., "Book Review: 'Telecommunications Network Management into the 21st Century'," *IEEE Communications*, Volume 32, No. 7, pp. 5-8, July 1994.

- Saidi, H., Min, P.S., and Hegde, M.V., "Guaranteed Cell Sequence in Nonblocking Multi-Channel Switching," *Proceedings of IEEE INFOCOM 94*, Toronto, pp. 1420-1427, June 1994.
- Min, P.S., Hegde, M.V., Saidi, H., and Chandra, A., "Shared Buffering in Nonblocking Copy Networks," *Proceedings of the 1994 IEEE International Symposium on Information Theory*, Norway, p. 406, June 1994.
- Min, P.S., Hegde, M.V., and Rayes, A., "Real Time Traffic Estimation in Circuit-Switched Networks," *Proceedings of the 14th International Teletraffic Congress*, France, pp. 1175-1184, June 1994.
- Hegde, M.V., Min, P.S., and Rayes, A., "State Dependent Routing: Traffic Dynamics and Performance Benefits," *Journal of Network and Systems Management*, Volume 2, No. 2, pp. 125-149, June 1994.
- Saidi, H., Min, P.S., and Hegde, M.V., "Control of Packet Flow in Statistical Data Forks," *Proceedings of the 1994 International Conference on Communications*, New Orleans, pp. 415-419, May 1994.
- Saidi, H., Min, P.S., and Hegde, M.V., "Nonblocking Multi-Channel Switching in ATM Networks," *Proceedings of the 1994 International Conference on Communications*, New Orleans, pp. 701-705, May 1994.
- Maunder, A. and Min, P.S., "Analysis and Development of Routing Schemes for Multi-Rate, Multi-Point Traffic," *Proceedings of the 1994 Conference on Information Sciences and Systems*, Princeton, pp. 1041-1046, March 1994.
- Min, P.S., Hegde, M.V., and Chandra A., "Internal Buffering in Banyan-Based Copy Networks," *Proceedings of the 1994 Conference on Information Sciences and Systems*, Princeton, pp. 209-214, March 1994.
- Rayes, A. and Min, P.S., "Capacity Expansion in State Dependent Routing Schemes," *Proceedings of the 1994 Conference on Information Sciences and Systems*, Princeton, pp. 237-241, March 1994.
- Vargas, C., Hegde, M.V., Naraghi-Pour, M., and Min, P.S., "Shadow Prices for State Dependent Routing," *Proceedings of the 1994 Conference on Information Sciences and Systems*, Princeton, pp. 243-248, March 1994.
- Saidi, H., Min, P.S., and Hegde, M.V., "Non-Blocking Multi-Channel Switching." Invited paper. *Proceedings of the 31st Annual Allerton Conference*, pp. 335-344, September 1993.
- Min, P.S., Hegde, M.V., and Rayes, A., "Model Based Estimation of Exogenous Traffic," *Proceedings of the 1993 Conference on Information Sciences and Systems*, Baltimore, pp. 126-131, March 1993.
- Hegde, M.V., Min, P.S., and Rayes, A., "Performance Analysis of State Dependent Routing," *Proceedings of the 1993 Conference on Information Sciences and Systems*, pp. 695-700, Baltimore, March 1993.
- Hegde, M.V. and Min, P.S., "Telephone Networks," Magill Survey of Science Applied Science, Salem Press, pp. 2624-2630, 1992.

- Saidi, H., Min, P.S., and Hegde, M.V., "Assignment of 2^k Trunk Groups in Multi-Channel Switches Using Generalized Binary Addresses," *Proceedings of the 30th Annual Allerton Conference*, pp. 652-661, September 1992.
- Hegde, M.V. and Min, P.S., "Performance Analysis of State Dependent Routing." Invited paper. *Second ORSA Telecommunications Conference*, Boca Raton, Florida, February 1992.
- Rizzoni, R. and Min, P.S., "Detection of Sensor Failures in Automotive Engines," *IEEE Transactions on Vehicular Technology*, Volume 40, No. 2, pp. 487-500, May 1991.
- Min, P.S. and Hegde, M.V., "End-to-End Planning Models for Optimal Evolution of Telecommunications Network," *Proceedings of IEEE INFOCOM 90*, San Francisco, pp. 200-206, June 1990.
- Min, P.S., "Validation of Controller Inputs in Electronically Controlled Engines." Invited paper. *Proceedings of the 1990 American Control Conference*, pp.2887-2890, San Diego, May 1990.
- Min, P.S. and Youn, C., "Generic Equipment Models (GEM) for Consistent Planning of Telecommunications Networks," *Proceedings of the 1990 ISMM International Conference*, New Orleans, pp. 190-194, March 1990.
- Min, P.S., "Robust Application of Beard-Jones Detection Filter," *Advances in Computing and Control*, Springer-Verlag, Volume 130, pp. 162-173, 1989.
- Min, P.S. and Ribbens, W.B., "A Vector Space Solution to Incipient Sensor Failure Detection," *IEEE Transactions on Vehicular Technology*, Volume 38, No.3, pp. 148-158, August 1989.
- Min, P.S., "Robust Application of Beard-Jones Detection Filter," *Proceedings of the 1989 American Control Conference*, Pittsburgh, pp. 859-864, June 1989.
- Rizzoni, G. and Min, P.S., "Real Time Detection Filters for the On-board Diagnosis of Incipient Failures," *Proceedings of the 1989 International Symposium on Allied Technology and Automation*, pp. 1445-1466, Paper No. 89131, Florence, Italy, June 1989.
- Min, P.S., "Diagnosis of On-Board Sensors in Internal Combustion (IC) Engines," *Proceedings of the 1989 American Control Conference*, Pittsburgh, pp. 1065-1070, June 1989.
- Min, P.S., "Detection of Incipient Sensor Failures in Internal Combustion Engines," *Proceedings of the 1988 International Symposium on Allied Technology and Automation*, Paper No. 88038, Florence, Italy, June 1988.

Testimony Provided or Expected to Provide as Expert Witness

Matter: Patent Infringement for Wireless Local Area Networks
Law Firm: Quinn Emanuel Urquhard & Sullivan LLP

Case Name: Certain Audio Players and Components thereof (II). U.S.I.T.C. Inv. No. 337-TA-1330.
Testifying Expert for Google Inc.
Completed in June 2023.
(Expert reports submitted and deposited.)

Matter: Patent Infringement for Wireless Communications
Law Firm: Alston & Bird
Case Name: Atlas Global Technologies LLC v. ASUSTek Computers Inc. USDC WD TX
Civil Action No. 6:21-cv-820
Testifying Expert for ASUSTek
Completed in November 2023
(Expert report submitted.)

Matter: Patent Infringement for Wireless Communications
Law Firm: Perkins Coie
Case Name: Bell Northern Research, LLC v. HMD AMERICA, INC. et al., Case No.: 1:22-cv-22706-SCOLA/GOODMAN (S.D. Fla.)
Testifying Expert for HMD
Completed in December 2023
(Expert report submitted. Deposed.)

Matter: Patent Infringement for Wireless Communications
Law Firm: LAW OFFICES S. J. CHRISTINE YANG
Case Name: Atlas Global Technologies LLC v. ZyXEL Communications Corp. et al.,
U.S.D.C., W.D.T.X., Waco Div., Case No. 6:22-cv-00355 Atlas Global
Technologies LLC v. D-Link Corp. U.S.D.C., W.D.T.X., Waco Div., Case No.
6:22-cv-00520
Testifying Expert for ZyXel
Retained in March 2023.
(Expert report submitted.)

Matter: Patent Infringement for Wireless Communications
Law Firm: Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
Case Name: Bell Northern Research v. MeidaTek Inc.
Testifying Expert for MediaTek Inc.
Retained in August 2023.

Matter: Patent Infringement for Home Security System
Law Firm: Foley and Lardner LLP
Case Name: Alarm.com v. Vivint, Inc., AAA Arbitration Case. No. 01-22-0004-5525 and
U.S.D.C. Case No. 2:23-cv-00004-JRG-RSP (E.D. Tex.),
Testifying Expert for Vivint, Inc.
Completed in 2023.

Matter: Patent Infringement for Wireless Communications and Electronics

Law Firm: Perkins Coie
Case Name: Bell Northern Research, LLC v. HMD AMERICA, INC. et al., Case No.: 1:22-cv-22706-SCOLA/GOODMAN (S.D. Fla.)
Testifying Expert for HMD
Completed in December 2023.

Matter: Patent Infringement for Network Switches
Law Firm: Charhon Callahan Robson & Garza, PLLC
Case Name: Sable Networks, Inc. and Sable IP, LLC v. CouldFlare, Inc. U.S.D.C. WD Tx
Case No. 6:21-cv-261
Testifying Expert for CloudFlare, Inc.
Completed in January 2024.
(Expert report submitted and deposed.)

Matter: Patent Infringement for Network Security
Law Firm: Fish and Richardson
Case Name: Finjan LLC v. Palo Alto Networks, Inc. – Case No. 4:14-cv-04908-PJH. USDC
ND CA, Oakland Division.
Testifying Expert for Finjan LLC.
Retained in September 2022.
(Expert report submitted and deposed.)

Matter: Patent Infringement for Network Management
Law Firm: Irell & Manella LLP
Case Name: SNMP Research, Inc. & SNMP Research International, Inc. v. Broadcom Inc.,
Brocade Communications Systems LLC, & Extreme Networks, Inc. U.S.D.C.
E.D. Tennessee at Knoxville Case No. 3:20-CV-451
Testifying Expert for SNMP Research.
Retained in May 2022.

Matter: Inter Parte Reexamination for Wireless Communications
Law Firm: Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
Case Name: Patent reexamination in front of the U.S.P.T.O.
Testifying Expert for MediaTek
Retained in March 2023.

Matter: Patent Infringement for Network Switching
Law Firm: Baker Botts
Case Name: Corrigent Corp. v. Arista Networks, Inc., Case No. 1:22-cv-00497-UNA. USDC
Delaware
Testifying Expert for Arista
Retained in October 2022.

Matter: Patent Infringement for Mobile Devices
Law Firm: Fish and Richardson
Case Name: GComm v. Samsung, U.S.D.C. ED. TX. Case No.:2:22-cv-0078-JRG

Testifying Expert for Samsung
Completed in January 2024.

Matter: Patent Infringement for Wireless Networks
Law Firm: McKool Smith
Case Name: Certain Mobile Telephones, Tablet Computers with Cellular Connectivity, and Smart Watches with Cellular Connectivity, Components Thereof, and Products Containing Same. U.S.I.T.C. Inv. No. 337-TA-1299
Testifying Expert for Ericsson
Completed in July 2022.
(Expert report submitted and deposed.)

Matter: Patent Infringement for Semiconductor Manufacturing
Law Firm: Kramer Levin
Case Name: Oasis Tooling, Inc. v. Siemens Indus. Software, Inc., 1:22-cv-151 (D. Del.), Oasis Tooling, Inc. v. GlobalFoundries U.S. Inc., 1:22-cv-312 (D. Del.)
Testifying Expert for Oasis Tooling
Retained in June 2022.
(Expert reports submitted.)

Matter: Patent Infringement for Optical Networks
Law Firm: Duane Morris
Case Name: NextGen Innovations, LLC v. Infinera Corporation. U.S.D.C. ED. TX (Marshall) Case No. 2:22-cv-00306-JRG-RSP / IPR
Testifying Expert for Infinera
Retained in April 2023.

Matter: Patent Infringement for Wireless Devices
Law Firm: King and Spalding LLP
Case Name: Intellectual Ventures, et. al. v. General Motors Company and General Company Motors, LLC, Case No. 6:21-CV-1088 pending in the Western District of Texas, Waco Division
Testifying Expert for General Motors
Completed in January 2023.
(Expert report submitted.)

Matter: Patent Infringement for Wireless Devices
Law Firm: Sterne Kessler
Case Name: Neo Wireless LLC v. Volkswagen Group of America, Inc. and Volkswagen Group of America Chattanooga Operations, LLC and related matters
Testifying Expert for Volkswagen
Completed in September 2023.
(Expert report submitted and deposed. IPR declarations submitted)

Matter: Patent Infringement for Wireless Networks
Law Firm: Covington & Burling LLP

Case Name: XR Communications, LLC v. D-Link Systems, Inc., No. 8:17-cv-00596
(Consolidated) (C.D. Cal.)
Testifying Expert for Hewlett Packard Enterprise
Completed
(Expert report submitted and deposited.)

Matter: Patent Infringement for USB Charging System
Law Firm: Orrick, Herrington & Sutcliffe LLP
Case Name: Fundamental Innovation Systems International LLC v. TCT Mobile (US), TCT
Mobile (US) Holdings, Inc., et al. U.S.D.C. Delaware No. 20-552-RGA-CJB
Testifying Expert for TCL
Completed in June 2022.
(Expert report submitted and deposited.)

Matter: Inter Parte Reexamination for Wireless Communications
Law Firm: Alston & Bird
Case Name: Patent reexamination in front of the U.S.P.T.O.
Testifying Expert for Nokia
Retained in May 2022.
(Expert report submitted.)

Matter: Patent Infringement for Network Management System
Law Firm: Morgan, Lewis & Bockius, LLP
Case Name: Certain Routers, Access Points, Controllers, Network Management Devices,
Other Networking Products, and Hardware and Software Components Thereof,
U.S.I.T.C. Inv. No. 337-TA-1227
Testifying Expert for Hewlett Packard, Netgear, and CommScope
Completed in August 2021.
(Expert report submitted, deposited, and testified during trial.)

Matter: Contract Dispute
Law Firm: Orrick, Herrington & Sutcliffe LLP
Case Name: Allied Telesis, Inc., et al vs. Micron Technology, Inc., Santa Clara County
Case No: 2015-1-CV-282977
Testifying Expert for Micron
Retained in 2021. Deposed in October 2021.
Completed in 2022

Matter: Patent Infringement for Security Systems
Law Firm: Forley and Lardner LLP
Case Name: Certain Residential Premises Security Monitoring and Automation Control
Panels, and Components Thereof (ITC Inv. No. 337-TA-1273) and ADT LLC et
al v. Vivint, Inc., Case No. 6:21-cv-00687 (W.D. Tex.)
Testifying Expert for Vivint, Inc.
Completed in April 2022.
(Expert report submitted, deposited, and testified during trial.)

Matter: Inter Parte Reexamination for Internet Communications

Law Firm: Perkins Coie

Case Name: Patent reexamination in front of the U.S.P.T.O.
Testifying Expert for Twitter
Retained in June 2020.
(Expert report submitted.)

Law Firm: Fisher Broyles

Case Name: Vaxcel International Co., Ltd. v. Heathco LLC, U.S.D.C. Delaware No. 20-224-LPS
Testifying Expert for Vaxcel
Retained in February 2021.
(Expert report submitted and deposed.)

Matter: Patent Infringement for Network Communication System

Law Firm: Charhon Callahan Robson & Garza, PLLC

Case Name: Sable Networks, Inc. and Sable IP, LLC, v. ClouFlare, Inc. U.S.D.C. WDTX, Civil Action No. 6:21-cv-261
Testifying Expert for CloudFlare, Inc.,
Completed in January 2024.

Matter: Patent Infringement for Mobile Wireless Device

Law Firm: Pearl Cohen

Case Name: In the Matter Of Certain UMTS And LTE Cellular Communications Modules And Products Containing The Same, U.S.I.T.C. Inv. No. 337-TA-1240
Testifying Expert for Telit Wireless Communication, Quectel, and Thales
Completed in March 2023.
(Expert reports submitted and deposed.)

Matter: Transactional Taxes for Internet Application

Law Firm: Ryan Rapp & Underwood, PLC

Case Name: ADP, LLC v. Arizona Department of Revenue (TX2018-000246),
Testifying Expert for ADP, LLC.
Completed in June 2020.
(Expert report submitted.)

Matter: Trade Secret Misappropriation in Digital Electronics

Law Firm: Goodwin Proctor LLP

Case Name: Guzik Technical Enterprises versus Keysight Technologies, Inc. Superior Court of the State of California for the County of Santa Clara, Case No.: 19CV355879
Testifying Expert for Keysight Technologies, Inc.
Retained in August 2020.

Matter: Patent Infringement for Fiber Optic Devices

Law Firm: Cooley

Case Name: Certain High-Density Fiber Optic Equipment and Components Thereof,
U.S.I.T.C. Inv. No. 337-TA-1194
Testifying Expert for AFL Communications, Panduit, FS.Com, Wirewerk, and
Siemon
Completed in October 2020.
(Expert reports submitted, deposed, and testified during trial.)

Matter: Patent Infringement for Optical Transport Networks
Law Firm: Venerble
Case Name: Huawei Technologies Co. Ltd v Verizon Communications, Inc., et. al., 2:20-cv-
0030
Testifying Expert for Verizon.
Retained in March 2020.
(IPR declarations submitted.)

Matter: Patent Infringement for Lighting System
Law Firm: Fisher Broyles
Case Name: Vaxcel International Co., Ltd., v. Jasco Products Company, LLC., (Case No.
USDC Western District of Oklahoma, 5:19-CV-00154-JD
Testifying Expert for Vaxcel.
Retained in August 2020.

Matter: Patent Infringement for Wireless Communication
Law Firm: McDermott Will & Emery
Case Name: Bell Northern Research LLC v. ZTE. (Case No. 3:18-cv-01786 - S.D. Cal)
Testifying Expert for ZTE.
Retained in July 2019.
(IPR declarations submitted.)

Matter: Patent Infringement for Wireless Communication
Law Firm: Jones Day
Case Name: Bell Northern Research LLC v. Kyocera Corp. (Case No. 3:18-cv-1785 - S.D.
Cal)
Testifying Expert for Kyocera.
Completed in May 2019.
(Claim construction declaration submitted, and deposed.)

Matter: Patent Infringement for Electronic Payment Systems
Law Firm: Paul Hastings
Case Name: ID Tech Corp. v. Samsung Electronics Co., Ltd., et al. (Case No. No. 8:17-cv-1748-
DOC-JDE (C.D. Cal))
Testifying Expert for Samsung.
Retained in January 2019.
(Expert reports submitted, and deposed.)

Matter: Patent Infringement for Internet Switching

Law Firm: Maynard Cooper
Case Name: Parity Networks, LLC v. Juniper Networks, Inc., Case No. 6:17-CV-00495-RWS-KNM (U.S.D.C.E.D. Tx.)
Testifying Expert for Juniper.
Retained in April 2018.
(IPR declarations submitted.)

Matter: Patent Infringement for Internet Switching
Law Firm: Morgan Lewis
Case Name: Parity Networks, LLC v. Hewlett Packard Enterprise Company, Case No. 6:17-CV-00682 (U.S.D.C.E.D. Tx.)
Testifying Expert for Hewlett Packard Enterprise Company.
Retained in September 2018.
(IPR declarations submitted.)

Matter: Inter Parte Rexamination for Covered Business Method
Law Firm: Reed Smith LLP
Case Name: NASDAQ v. Miami International
Expert for Miami International.
Retained in February 2018.
(Expert declarations submitted, and deposited.)

Matter: Patent Infringement for Mobile Devices
Law Firm: Quinn Emanuel
Case Name: Qualcomm v. Apple, Case No. 3:17-cv-00108-GPC-MDD (U.S.D.C.S.D. Cal.)
Testifying Expert for Qualcomm.
Completed in April 2019.
(Expert reports submitted, and deposited.)

Matter: Patent Infringement for Communication Devices
Law Firm: Venable
Case Name: Sycamore IP Holdings LLC v. Verizon Communications Inc, Case No. 2:16-cv-591-JRG-RSP (U.S.D.C. E.D. Texas)
Testifying Expert for Verizon and Level 3.
Completed in September 2017.
(Expert reports submitted, and deposited.)

Matter: Patent Infringement for Mobile Devices
Law Firm: Alston Bird
Case Name: Huawei Technologies Co. Ltd. V. Nokia Solutions and Networks, Case No. 2:16-cv-0056-JRG-RSP (U.S.D.C. E.D. Texas)
Testifying Expert for Nokia.
Completed in December 2017.
(Expert reports submitted.)

Matter: Patent Infringement for Mobile Devices
Law Firm: Quinn Emanuel
Case Name: Huawei Technologies Co. Ltd. V. Samsung Electronics C. Ltd, Case No. 3:16-cv-02787 (U.S.D.C. N.D. Cal)
Testifying Expert for Samsung.
Completed in March 2019.
(Expert reports submitted, and deposed.)

Matter: Arbitration for Licensing
Law Firm: Alston Bird
Case Name: Nokia v. LG Electronics, International Chamber of Commerce Arb. No. 21326
Testifying Expert for Nokia.
Completed in October 2016.
(Expert reports submitted.)

Matter: Patent Infringement for Mobile Devices
Law Firm: Ropes and Gray
Case Name: Godo Kaisha IP Bridge 1 v. TCL Communication Technology Holdings, Case No. 15-634-SLR-SRF (U.S.D.C.S.D. Delaware.)
Testifying Expert for IP Bridge.
Completed in October 2018.
(Expert reports submitted, and deposed.)

Matter: Patent Infringement for Mobile Devices
Law Firm: Paul Hastings
Case Name: Odyssey Wireless, Inc., v. Samsung Electronics Co., Ltd., et al, Case No. 3:15-cv-1738-H-RBB (U.S.D.C.S.D. Cal.)
Testifying Expert for Samsung.
Completed in October 2016.
(Expert reports submitted.)

Matter: Patent Infringement for Mobile Devices
Law Firm: Greenberg Traurig
Case Name: Mobile Telecommunications Technologies LLC v. Amazon.com, Inc., 2:13-cv-883-JRG-RSP (U.S.D.C. E.D. Texas)
Testifying Expert for Amazon.
Completed in April 2015.
(Expert reports submitted, and deposed.)

Matter: Patent Infringement for Mobile Devices
Law Firm: Mayer Brown
Case Name: Mobile Telecommunications Technologies LLC v. LG Electronics Mobilecomm U.S.A., Inc., 2:13-cv-947-JRG-RSP (U.S.D.C. E.D. Texas)
Testifying Expert for LG Electronics Mobilecomm.
Completed in February 2016.
(Expert reports submitted, and deposed.)

Matter: Patent Infringement for Semiconductor Devices
Law Firm: Mayer Brown
Case Name: Inter Parte Reexamination for U.S. Patent Nos. 6,895,520 and 6,899,332
Expert for LG Electronics.
Completed in February 2016.
(Expert declaration submitted, and deposed.)

Matter: Patent Infringement in Vehicular Electronics
Law Firm: Gardner, Linn, Burkhardt & Flory, L.L.P
Case Name: *Magna Electronics Inc. v. TRW Automotive Holdings Corp. et al.*, Civil Action No. 1:12-cv-00654 (Western District of Michigan), and relating to the action styled *Magna Electronics Inc. v. TRW Automotive Holdings Corp. et al.*, Civil Action No. 1:13-cv-00324 (Western District of Michigan).
Testifying Expert for Magna Electronics
Completed in February 2016.
(Expert reports submitted, and deposed.)

Matter: Patent Infringement in Electronic Circuits
Law Firm: Ropes and Gray
Case Name: Certain Devices Containing Non-Volatile Memory and Products Containing the Same (USITC Inv. Nos. 337-TA-922)
Testifying Expert for Spansion Inc.
Completed in February 2015.
(Expert reports submitted.)

Matter: Trade Secret Misappropriation in Software Method for Cable Television Advertisement
Law Firm: Brownstein Hyatt Farber Schreck
Case Name: Cross MediaWorks v. EMT Holdings, USDC Southern District of New York, Case No. 1:14-cv-00561-VSB
Testifying Expert for Cross MediaWorks.
Completed in April 2015.
(Testified during injunction hearing.)

Matter: Patent Infringement in Vehicular Electronics
Law Firm: Steptoe and Johnson
Case Name: Certain Vision-Based river Assistance System Cameras and Components Thereof (USITC Inv. Nos. 337-TA-899 and 907)
Testifying Expert for Magna Electronics
Completed in February 2015.
(Expert reports submitted, deposed, and testified during trial.)

Matter: Patent Infringement for Vehicular System
Law Firm: Susman Godfrey

Case Name: Eagle Harbor Holdings, LLC, and Mediustech, LLC, v. Ford Motor Company, 3:11-cv-05503-BHS (U.S.D.C. Western District of Washington at Tacoma)
Testifying Expert for Mediustech.
Completed in March 2015.
(Expert reports submitted, deposed, and testified during trial.)

Matter: Patent Infringement for Communication Networks
Law Firm: Davis Polk & Wardwell LLP
Case Name: Sprint Communications Company L.P., v. Comcast Cable Communications, LLC, Comcast IP Phone, LLC, and Comcast Phone of Kansas, LLC. 2:11-cv-02684-KHV-DJW (U.S.D.C. Kansas)
Testifying Expert for Comcast.
Retained in March 2012.
(Expert reports submitted, and deposed.)

Matter: Patent Infringement for Communication Networks
Law Firm: Quinn Emanuel
Case Name: France Telecom S.A. v. Marvell Semiconductor, Inc., 12-Civ-4986 (S.D.N.Y.)
Testifying Expert for Marvell.
Completed in September 2014.
(Expert reports submitted, deposed, and testified during trial.)

Matter: Wireless Image Distribution
Law Firm: Jones Day
Case Name: *Inter Partes* Review of U.S. Patent No. 8,437,797
Expert for Google Inc.
Completed in November 2014.
(Expert declaration submitted.)

Matter: Nonvolatile Semiconductor Memories
Law Firm: Jones Day
Case Name: *Inter Partes* Review of U.S. Patent Nos. 8,301,833 and 8,516,187
Expert for SanDisk.
Completed in May 2014.
(Expert declaration submitted.)

Matter: Communication Protocols for Wireless Device
Law Firm: Dorsey & Whitney, LLP
Case Name: Certain Point-To-Point Network Communication Devices and Products Containing Same (USITC Inv. No. 337-TA-892)
Testifying Expert for Toshiba
Completed in May 2014.
(Expert reports submitted, and deposed.)

Matter: Patent Infringement for Wireless Networks
Law Firm: Ropes and Gray

Case Name: In the Matter of Certain Wireless Devices With 3G and/or 4G Capabilities and Components Thereof (USITC Inv. No. 337-TA-868) InterDigital Comms., Inc. v. Huawei Techs. Co., Ltd., No. 13-00008 (D. Del., filed January 2, 2013), InterDigital Comms., Inc. v. ZTE Corp., No. 13-00009 (D. Del., filed January 2, 2013), InterDigital Comms., Inc. v. Nokia Corp., No. 1:13-cv-00010 (D. Del., filed January 2, 2013), InterDigital Comms., Inc. v. Samsung Elec. Co., Ltd., No. 13-00011 (D. Del., filed January 2, 2013)
Testifying Expert for Joint Defense Group.
Completed in February 2014.
(Expert reports submitted, deposed, and testified during trials.)

Matter: Patent Infringement for Mobile Communication
Law Firm: Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P.
Case Name: Certain Digital Media Devices, Including Televisions, Blu-Ray Disc Players, Home Theater Systems, Tablets and Mobile Phones, Components Thereof and Associated Software (USITC Inv. No. 337-TA-882)
Testifying Expert for LG Electronics, Inc.
Completed in February 2014.
(Expert reports submitted, deposed, and testified during trial.)

Matter: Patent Infringement for Wireless Networks
Law Firm: Vinson & Elkins LLP
Case Name: Wi-LAN USA, Inc. and Wi-LAN, Inc. v. Telefonaktiebolaget LM Ericsson and Ericsson, Inc. (USDC: Southern District of FL - Case #1: 12-cv-23569), Wi-LAN USA, Inc. and Wi-LAN, Inc. v. Alcatel-Lucent USA, Inc. (USDC: Southern District of FL - Case #1: 12-cv-23568-Altonaga/Simonton)
Testifying Expert for Wi-LAN.
Completed in May 2015.
(Expert reports submitted, and deposed.)

Matter: Patent Infringement for Data Storage
Law Firm: Ropes and Gray, Weil Gotshal
Case Name: Summit Data Systems, LLC v. EMC Corporation., et al. 1:10-cv-00749-GMS (U.S.D.C. Delaware)
Testifying Expert for EMC Corporation and Netapp, Inc.
Completed in December 2012.
(Expert reports submitted, and deposed.)

Matter: Patent Infringement for Wireless Mobile Device
Law Firm: Ashurst Australia
Case Name: Samsung v. Apple, Australian Federal Court Proceeding No. NSD 1243 of 2011
Testifying Expert for Samsung Electronics.
Completed in December 2012.
(Expert reports submitted, deposed, and testified during trial.)

Matter: Patent Infringement for Wireless Mobile Devices

Law Firm: Quinn Emanuel
Case Name: Apple Inc. v. Samsung Electronics Co., Ltd., et al., 4:11-cv-01846-LHK (N.D. Cal.) and Samsung Electronics Co., Ltd., et al. v. Apple Inc., 4:11-cv-02079 (N.D. Cal.)
Testifying Expert for Samsung Electronics.
Completed in July 2012.
(Expert reports submitted, and deposed.)

Matter: Patent Infringement for Wireless Mobile Device
Law Firm: Quinn Emanuel
Case Name: Certain Electronic Devices, Including Wireless Communication Devices, Portable Music And Data Processing Devices, And Tablet Computer, U.S.I.T.C. Inv. No. 337-TA-794
Testifying Expert for Samsung Electronics.
Completed in June 2012.
(Expert reports submitted, deposed, and testified during trial.)

Matter: Patent Infringement for Portable Storage Device
Law Firm: White and Case
Case Name: CERTAIN UNIVERSAL SERIAL BUS (“USB”) PORTABLE STORAGE DEVICES, INCLUDING USB FLASH DRIVES AND COMPONENTS THEREOF, US International Trade Commission Investigation No. 337-TA-788
Testifying Expert Witness for Trek
Completed in May 2012.
(Expert reports submitted, and deposed.)

Matter: Copyright Infringement for Petroleum Processing Software
Law Firm: Osha Liang LLP
Case Name: Aspen Technology, Inc. v. Tekin A. Kunt and M3 Technology, Inc., Case Number: H-10-1127, US District Court, Texas, Houston Division.
Testifying Expert for M3 Technology, Inc.
Completed in May 2012.
(Expert reports submitted, deposed, and testified during trial.)

Matter: Trade Secret Misappropriation for DC-DC converter
Law Firm: Covington & Burling, Haynes Boone
Case Name: Certain DC—DC Controllers and Products Containing Same, US International Trade Commission Investigation No. 337-TA-698
Testifying Expert for UPI.
Completed in March 2012.
(Expert reports submitted, deposed, and testified during trial.)

Matter: Patent Infringement for Parallel Processor
Law Firm: Orrick, Herrington, & Sutcliffe. Kirkland and Ellis.
Case Name: BIAx Corporation v. Nvidia and Sony Civil Action No. 09-cv-01257-PAB-MEH
Testifying Expert for Nvidia and Sony

Completed in March 2012.
(Expert reports submitted, and deposed.)

Matter: Patent Infringement for Call Center Technology
Law Firms: Duffy, Sweeney, and Scott. Foley Lardner.
Case Name: Ronald Katz Technology Licensing v. Citizens Financial Group 7-ML-1816-C
RGK (FFM)
Testifying Expert Witness for Citizens Financial Group.
Completed in 2011.
(Expert reports submitted, and deposed.)

Matter: Patent Infringement for Storage Area Network
Law Firm: DLA Piper
Case Name: Network Appliance, Inc., v. Sun Microsystems, Inc., Case Number: C-07-06053
EDL, US District Court, Northern District of California, San Francisco Division.
Testifying Expert for Sun Microsystems, Inc.
Completed in 2010.
(Expert reports submitted, and deposed.)

Matter: Patent Infringement for Flat Panel Display Controller
Law Firm: Jones Day
Case Name: Certain Video Displays, Components Thereof, and Products Containing Same, US
International Trade Commission Investigation No. 337-TA-687
Testifying Expert for Vizio, Inc.
Completed in 2010.
(Expert reports submitted, deposed, and testified during trial.)

Matter: Patent Infringement for Call Center Technology
Law Firms: Foley Lardner
Case Name: Ronald Katz Technology Licensing v. US Bank 7-ML-1816-C RGK (FFM)
Testifying Expert Witness for US Bank
Completed in May 2009.
(Expert reports submitted, and deposed.)

Matter: Patent Infringement for USB to VGA Converter
Law Firm: Wang Hartmann, Gibbs, & Cauley, P.C.
Case Name: Displaylink Corporation v. Magic Control Technology Corporation, Case No.
5:07-CV-01998-RMW, US District Court, Northern District of California, San
Francisco Division.
Testifying Expert for Magic Control Technology Corporation
Completed in 2009.
(Expert reports submitted, and deposed.)

Matter: Patent Infringement for Flash Memory
Law Firm: Jones Day and Wilson Sansini

Case Name: Certain Flash Memory Controllers, Drives, Memory Card, and Media Players and Products Containing Same. US International Trade Commission Investigation No. 337-TA-619

Testifying Expert for SanDisk Corporation.

Completed in 2008.

(Expert reports submitted, deposed, and testified during trial.)

Matter: Patent Infringement for Semiconductor Packaging

Law Firm: Jones Day

Case Name: Certain Semiconductor Chips with Minimized Chip Package Size and Products Containing the Same. US International Trade Commission Investigation No. 337-TA-605

Testifying Expert for Freescale Semiconductor

Completed in 2008.

(Expert reports submitted, deposed, and testified during trial.)

Matter: Patent Infringement for Automatic Switching System

Law Firms: Jones Day, and Heller Ehrman, LLP.

Case Name: ATEN International Co., Ltd and ATEN Technology, Inc. v. Belkin Corporation, Belkin Logistics, Inc. and Emine Technology Co., Ltd. US International Trade Commission Investigation No. Ltd 337-TA-589

Testifying Expert for Belkin Corporation, Belkin Logistics, Inc., and Emine Technology Co., Ltd.

Completed in 2007.

(Expert reports submitted, deposed, and testified during trial.)

Matter: Patent Infringement for Dual Mode Communication

Law Firm: Wilmer Cutler Pickering Hale and Dorr, LLP

Case Name: Broadcom Corporation v. Qualcomm Incorporated SACV05-467-JVS (RNBx)

Testifying Expert Witness for Broadcom Corporation

Completed in 2007.

(Expert reports submitted, deposed, and testified during trial.)