UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

***Inter Partes* Review**

Cisco Systems, Inc.,
Petitioner,
v.

Lionra Technologies Limited,
Patent Owner.

IPR2024-00734
U.S. Patent No. 7,632,518

DECLARATION OF DR. ERIC COLE IN SUPPORT OF PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I. INTRODUCTION 1

II. QUALIFICATIONS 2

III. SCOPE OF WORK 8

IV. LEVEL OF ORDINARY SKILL IN THE ART 9

V. LEGAL PRINCIPLES 10

A. Anticipation 10

B. Obviousness 13

VI. OVERVIEW OF THE CHALLENGED PATENT 16

A. Assumed Effective Filing and Invention Dates 16

B. The Challenged Patent 16

VII. A POSITA Would Not Have Been Motivated To Combine The Gai, Yip and/or Kwan References On April 8, 2004. 21

VIII. A POSITA Would Not Have Been Motivated To Combine The Gai, Yip, Kwan and Georgiou References On April 8, 2004. 34

IX. The Non-Volatile Random Access Memory (NVRAM) 408, Dynamic Memory 409, and TCAM 410 Disclosed in Gai Do Not Meet the Limitation of a "Memory Circuit Coupled to the Forwarding Circuit" recited in claims 15 and 19. 38

I, Eric Cole, of Ashburn, Virginia, declare that:

I. INTRODUCTION

1. Lionra Technologies Limited has retained me as an independent expert in connection with IPR2024-00734 to provide testimony regarding the technology involved in U.S. Patent No. 7,623,518 (the "'518 Patent," or the "Challenged Patent") and how the inventions described and claimed therein compare with the asserted prior art. I have been asked to provide my technical review, analysis, insights, and opinions regarding the references set forth in the above-referenced IPR by Petitioner Cisco Systems.

2. I am being compensated for my work in this matter at my standard hourly rate for consulting services at $700 per hour. My compensation is not dependent on the outcome of the case and does not affect the substance of my statements in this Declaration. I have no financial interest in the matter or the patent at issue.

3. I have reviewed the specification and the claims of the '518 patent, as well as the prosecution history for the patent. I am familiar with the technology involved therein, having practical, hands-on experience in the field for over 30 years.

II. QUALIFICATIONS

4. My academic credentials include a master's degree in computer science and a doctorate in information security, and I have worked in the cyber and technical information security industry for over twenty-five years. The details of my education and experience are summarized in my curriculum vitae ("CV"), which is attached as Exhibit 2002. My CV also includes a list of my publications over the past ten years.

5. I have worked in computer security for over twenty-five years. To briefly summarize my career, I have: 1) been responsible for the security of sensitive government projects; 2) managed security at major private sector companies; 3) consulted for major private sector companies; 4) been actively involved in designing, building, and deploying intrusion detection systems; 5) worked on protecting and securing critical information including trade secrets; 6) continually taught and written about cybersecurity.

6. I am the founder and president of Secure Anchor Consulting, LLC, located in Ashburn, Virginia. Secure Anchor Consulting provides cybersecurity consulting services and leads research and development initiatives to advance information systems security. Many of the clients I work with are responsible for

protecting sensitive client and/or consumer information and implementing effective security.

7. At Secure Anchor Consulting, I also actively work on incidents, and I have a detailed understanding of measures that organizations can take to both prevent and detect breaches. In addition, I have worked with organizations to design, build, and implement security measures that would be classified as both fixes and compensating controls, and I have detailed knowledge of the effort that is required to implement various remediation measures.

8. I worked for the U.S. government for eight years as an employee and have held various contracting jobs with government agencies, which involved working with classified information. I have worked for a wide range of government organizations, including the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the Central Intelligence Agency (CIA), the Department of Energy, the Department of Defense (DOD), the Treasury Department, the Secret Service, and the Nuclear Regulatory Commission (NRC). I have held various top-secret security clearances with the DOD, the CIA, and the NRC. I also was involved in funded research from the Defense Advanced Research Projects Agency (DARPA), an agency of the DOD responsible for the development of new intrusion detection technologies for use by the military. During this time, I have reviewed,

edited, and created numerous security policies. On several occasions, I have also reviewed the reasonableness of measures intended to protect and secure Confidential Information through various types of documentation to include policies, procedures, standards, and baselines.

9. While serving as a Senior Officer for the CIA as Program Manager / Technical Director for the Internet Program Team with the Office of Technical Services, I implemented the Internet Program Team that designs, develops, tests, and deploys internet security products in three- to six-month intervals. In this role, I received a letter of appreciation from the Director of Central Intelligence and six Exceptional Performance Awards.

10. As a member of the Information Security Assessment Team with the Office of Security at the CIA, I evaluated and performed security assessments of network operating systems to identify potential vulnerabilities and solutions. I also designed a large-scale auditing system with an automated review capability and worked on several virus investigations for the Office of Security.

11. In my role as Chief Information Officer for the American Institutes for Research, I repaired and developed IT infrastructures for various organizations. I was also responsible for building out the entire data classification program to ensure that critical and proprietary data was properly protected and secured. I was also one

of the principal leads on research funding from DARPA. In this role, I was responsible for understanding the current state of the art in intrusion detection and designing and building a new cybersecurity system that could catch attacks that were targeting organizations.

12. As Chief Scientist and Senior Fellow for Lockheed Martin, I performed research and development in information systems security. I also specialized in evaluating and designing secure network design, perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems. At Lockheed Martin, I served as a technical advisor in high-profile security projects for government clients including the DOD, the FBI Sentinel case management systems, Department of Homeland Security Enterprise Acquisition Gateway for Leading Edge solutions, Jet Propulsion Labs, Hanford Labs, and FBI Information Assurance Technology Infusion programs.

13. As Chief Technical Officer for McAfee, I executed the strategy for technology platforms, partnerships, and external relationships to establish product vision and achieve McAfee's goals and business strategies. In this capacity, I worked closely with groups tasked with the development of intellectual property. While at McAfee, I worked with many business customers responsible for protecting clients' information, helping them implement effective security solutions.

14. I was a fellow and instructor for twenty years with the SANS Institute, a research and education organization consisting of information security professionals. SANS is the largest source for information security training and security certifications in the world. I am an author of several security courses, such as SEC401-Security Essentials and SEC501-Enterprise Defender. SEC401-Security Essentials is a required course for agents of the FBI and the NSA. These courses have been taken by over 30,000 people, and I have taught more than 50% of these students via live and online training. The courses that I have written have multiple modules and lessons on security policies, employee agreements, and protection of intellectual property. As one of the top-rated instructors at SANS, I have delivered keynote addresses around the world.

15. I am a member of the European InfoSec Hall of Fame, a professional membership awarded by nomination and election by a panel of industry experts.

16. I hold a Certified Information System Security Professional (CISSP) certification and was the creator of the Global Information Assurance Certification (GIAC) Security Essentials Certification (GSEC).

17. I am a contributing author of "Securing Cyberspace for the 44th President" and served as a Commissioner on cybersecurity for President Obama. My Nine books on cybersecurity include "Online Danger," "Network Security Bible -

2nd Edition," "Advanced Persistent Threat," and "Insider Threat," which have become recognized as industry-standard sources. They are used in many classrooms and colleges around the world as authoritative texts on cybersecurity. I have also published several articles in the field.

18. The focus of my work over the last ten years has been on data protection for commercial organizations. I am very familiar with best practices in cybersecurity and have developed many of the standard practices.

19. Today, my consulting efforts help organizations properly protect client information and relate to various alternative methods of security that can be implemented. This includes hardening of systems, securing servers, proper configuration, patching, and compensating controls. In cases where a fix cannot be made because it would negatively impact the business, I have extensive experience in understanding various compensating controls as an alternative to minimize the risk to an acceptable level and how to implement those controls.

20. I routinely help clients develop and implement company-wide policies, training, and best practices to prevent potential cybersecurity incidents. My work addresses threats from both internal and external sources, including accidental and intentional incidents.

21. I have led, and been involved in working on, responses to many cybersecurity incidents. This includes performing root cause analysis, verifying the reasonableness of security measures, and validating the implementation of additional remediation measures.

22. In my consulting work and in the various positions that I have held, I have been responsible for protecting organizations to minimize and prevent data breaches, in addition to responding to breaches post detection. I have a very detailed understanding of what is and is not a reasonable level of security based on the hundreds of organizations with which I have worked and the various security task forces with which I have been involved.

III. SCOPE OF WORK

23. I have been asked to consider and provide my opinions on the claims of the Challenged Patent, including the technical subject matter and the application of various references that predate the priority date of the Challenged Patent. In particular, I have been asked to consider what one of ordinary skill in the art would have understood from the claims and specification of the Challenged Patent, and whether certain references would have disclosed or suggested the features recited in the claims of the Challenged Patent to a person of ordinary skill in the art at the time of filing of the Challenged Patent.

24. I am compensated at a rate of $700/hour for my work. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of any proceeding.

25. My opinions set forth below are based on my education, training, experience, and the content of the references considered.

IV. LEVEL OF ORDINARY SKILL IN THE ART

26. My opinions are provided based on what a person of ordinary skill in the art in the technical field of the inventions of the Challenged Patent would have understood at the time of filing of the Challenged Patent.

27. I have been informed and understand that the content of a patent and prior art should be interpreted the way a person of ordinary skill in the art would have interpreted those references at the time of filing of the patent. I understand that the person of ordinary skill is a hypothetical concept referring to one who understands the technology and associated conventional wisdom at the time.

28. I was asked to provide an opinion as to the level of one of ordinary skill in the art pertinent to the subject matter set forth in the Challenged Patent at the time of the priority date. Around April 8, 2004 (the filing date of patent application 10/822,048), it is my opinion that a person of ordinary skill in the art in the field of the Challenged Patent would have been a person with a Bachelor's degree in

computer science, computer engineering, electrical engineering or equivalent and at least two years of experience in computer networking and network system security. Throughout this declaration, I use the term "POSITA" to refer to a person with these or similar qualifications. To have similar qualifications, an individual with additional education or additional industrial experience could still be of ordinary skill in the art if that additional education or experience compensates for a deficit in one of the other aspects of the requirements stated above.

29. The basis for my familiarity with the level of ordinary skill is my interaction with large numbers of workers in the computer security industry who were at this level of skill. In reaching this opinion as to the hypothetical person of ordinary skill in the art, I have considered the types of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level and professional capabilities of workers in the field. I further note that, as of April 8, 2004, I was at least at this level of skill.

V. LEGAL PRINCIPLES

A. Anticipation

30. I understand and have been informed that in order for an inventor to be entitled to a patent, the invention must be "new," and the inventor must not have lost

his or her right to a patent by delaying filing of a patent application directed to the invention. There are a number of ways that an invention can be "anticipated"—that is, not new.

31. One such way is when the invention was already patented or described in a printed publication anywhere in the world before the date of invention by the inventor or more than one year before the earliest effective filing date of the patent application. Additionally, a patented invention may not be new if it was on sale or publicly used more than one year before the filing of an application for patent. A patented invention is also not new if it was "known" or used by others in the United States before it was invented by the patent applicants. To invalidate a patent claim based on knowledge, I understand that the knowledge must be accessible to the public. If the subject matter covered by a patent claim is found within the "four corners" of a prior art reference, the claim is said to be anticipated by that reference.

32. A patent claim can be said to be anticipated if each and every limitation of the patent claim is found either expressly or inherently in a single item of prior art. While a prior art reference need not use the same words as a patent claim to anticipate the claim, the prior art reference must describe the requirements of the claim with sufficient clarity such that a POSITA would have been able to make and

use the claimed invention based on the reference and his or her knowledge in the applicable technical field.

33. The disclosure of a feature of a claimed invention can be either "express," meaning that the text, figures, or other content of a reference actually teaches the aspects of the patent claim, or the disclosure can be "inherent." An express disclosure does not need to use the same words as the patent claim being considered and does not need to be depicted in exactly the same way, but the disclosure must actually convey the claimed invention to a POSITA using some combination of words, figures, data, or other portions of the patent. I have been informed and understand that in order to establish that an element of a claim is "inherent" in the disclosure in a prior art reference, it must be clear to a person skilled in the art that the missing element is an inevitable part of what is explicitly described in the reference, and that it would have been recognized as necessarily present by a person skilled in the art. Inherency cannot be established by probabilities or possibilities, and the mere fact that something may result from a given set of circumstances is not enough to establish inherency.

34. Finally, I further understand that to anticipate a claim, the elements of the claim must be found in the prior art reference "arranged as in the claim." I have been informed that this means that the elements of the prior art reference may not be

recombined in a way that is not taught in the prior art to arrive at the invention; instead, the prior art must teach the claimed subject matter in the arrangement required by the claims.

35. I understand that any disclosure that anticipates a claim also renders that claim obvious.

36. I have been informed and understand that a claim in dependent form shall contain a reference to a claim previously set forth and then specify a further limitation of the subject matter claimed and that a claim in dependent form shall be construed to incorporate by reference all the limitations of the claim to which it refers.

B. Obviousness

37. I have been informed and understand that subject matter claimed in a patent is obvious under 35 U.S.C. § 103 if a person of ordinary skill in the art at the time the alleged invention was made would have had reason to combine or modify the disclosures of one or more prior art references to arrive at the claimed subject matter. A claim may be unpatentable even if each and every claim limitation is not present or disclosed in a single prior art item.

38. I have been informed and understand that, under the doctrine of obviousness, a claim is unpatentable if the differences between the invention and the

prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. A person of ordinary skill in the art is presumed to have knowledge of the relevant prior art at the time of the claimed invention.

39. I have been informed and understand that obviousness is based on the scope and content of the prior art, the differences between the prior art and the claim, the level of ordinary skill in the art, and secondary indicia of obviousness and non-obviousness to the extent such indicia exist.

40. I have been informed and understand the determination of whether the asserted claims would have been obvious to a person of ordinary skill in the art and, therefore, invalid is not governed by any rigid test or formula. A determination that a claim is obvious is, instead, based on a common-sense determination that the claimed invention is merely a combination of known limitations to achieve predictable results. Any of the following rationales are acceptable justifications to conclude that a claim would have been obvious: (1) the claimed invention is simply a combination of known prior art methods to yield predictable results; (2) the claimed invention is a simple substitution of one known element for another to obtain predictable results; (3) the claimed invention uses known techniques to improve similar devices (methods or products) in the same way; (4) the claimed

Lionra Technologies Ltd.
Ex. 2001 - Page 16

invention applies a known technique to a known device (method or product) ready for improvement to yield predictable results; (5) the claimed invention was "obvious to try"—choosing from a finite number of identified, predictable solutions with a reasonable expectation of success; (6) there is known work in one field of endeavor that may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; or (7) there is some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference to combine prior art teachings to arrive at the claimed inventions.

41. I have been informed and understand that a claim may be obvious in light of a single reference, without the need to combine references, if the elements of the claim that are not found in the reference can be supplied by the common sense or knowledge of one of ordinary skill in the art or taught in different areas of the single reference.

42. I have been informed and understand that an analysis of whether a claimed invention is obvious must not rely on a hindsight combination of prior art. The analysis must proceed in the context of the time of the invention or claimed priority date and consider whether the invention as a whole would have been obvious

to a person of ordinary skill in the art, taking into consideration any interrelated teachings of the prior art, the effects of demands known to the design community or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine any known elements in the fashion claimed by the patent at issue.

VI. OVERVIEW OF THE CHALLENGED PATENT

A. Assumed Effective Filing and Invention Dates

43. The ’518 Patent is entitled “Dynamic Access Control Lists” and was filed on April 8, 2004. *See* Ex. 1001. I assume the priority date for the Challenged Patent is the filing date of the patent application, April 8, 2004.

B. The Challenged Patent

44. As noted in the Background of the Invention section of the Challenged Patent, “[i]n an Ethernet local area network (LAN), computers or hosts are attached to the network and each host is uniquely identified by a physical address which is designated a media access control (MAC) address in an Ethernet network. The MAC address of each host is typically hardwired into an Ethernet network interface card in the host. The network interface card in each host transmits and receives Ethernet packets to communicate with the other hosts in the network. Each Ethernet packet

includes an address segment including the MAC address of the host to receive the packet (destination MAC address) along with the MAC address of the host sending the packet (source MAC address), and further includes a data segment, as will be understood by those skilled in the art. The MAC address of each host is utilized by Ethernet switches in the network to receive and forward Ethernet packets between hosts. More specifically, a switch receives an Ethernet packet from a source host, examines the destination MAC address portion of the packet to determine where to forward the packet, and forwards the packet to the host corresponding to the destination MAC address." Ex. 1001, 1:5-24.

45. As further noted, "[i]n many situations, an Ethernet network must communicate with hosts outside the network and in different types of networks. For example, a user of a host in an Ethernet network may want to access various Web sites and Web pages contained on the Internet. To communicate with other types of networks, the host utilizes the Internet Protocol (IP) which allows hosts in many different types of networks to communicate with each other through IP packets. Within the Ethernet network, each host must be assigned an IP address by a network administrator for the purpose of communicating with computers outside the network via the Internet Protocol." *Id.*, 1:25-35.

46. Devices known as routers operate to forward IP packets from one network to another utilizing the IP addresses contained in the IP packets being communicated." A router typically includes an access control list (ACL) to restrict or define the hosts with which a given host is allowed to communicate. … [A]ccess control lists are utilized as a tool for network security to define or control the hosts and other objects, such as files and directories, with which a given host can communicate. For example, IP packets from a particular IP network or a particular Web site may be restricted from being received by hosts in the Ethernet network. In this situation, the access control list on the router would contain a field indicating that packets from the IP address corresponding to this Web site are to be denied, meaning that any such packets received by the router will not be forward to the intended host in the Ethernet network. IP packets include source and destination IP addresses, with the source IP address corresponding to the IP address of the host that sent the packet and the destination IP address corresponding to the host that is to receive the packet. *Id.*, 1:36-57.

47. The inventor of the Challenged Patent recognized that "[t]here is a need for access control lists that allows access of hosts in a computer network such as an Ethernet network to be restricted or controlled based upon user names, MAC

addresses, domain names, and DNS names instead of merely IP address information." *Id.*, 3:12-16.

48. The Challenged Patent discloses an Ethernet switch according to an embodiment of the claimed inventions using a functional block diagram in Figure 3. *Id.*, 4:42-44. In the embodiment corresponding to challenged apparatus claims 15 and 19, "[t]he switch 102 further includes a direct memory access (DMA) controller 304 that transfers the packets selected by the switch forwarding engine 300 to a packet memory 306. The selected packets are stored in the packet memory 306 for processing by the processor 302. Also stored in either the packet memory 306 … is the enhanced access control list 108 (FIG. 2) along with required programming instructions for execution by the processor to control the overall operation of the switch 102. To store a selected packet from the switch forwarding engine 300, the processor 302 programs required registers in the DMA controller 304. The switch forwarding engine 300 then supplies the packet to the DMA controller 304 which, in turn, stores the packet in the packet memory 306. The processor 302 accesses the stored packets in the packet memory 306 along with the stored enhanced access control list 108 (FIG. 2) to generate the dynamic access control list 104 (FIG. 2). After the processor 302 processes a given packet stored in the packet memory 306, the packet may need to be provided to the intended destination host 106. To forward

a packet stored in the packet memory 306 to the intended destination host 106, the processor 302 addresses the packet memory to access the desired packet and programs required registers in the DMA controller 304. In response to being programmed, the DMA controller 304 reads the accessed packets from the packet memory 306 and supplies these packets to the switch forwarding engine 300…." *Id.*, 9:28-55.

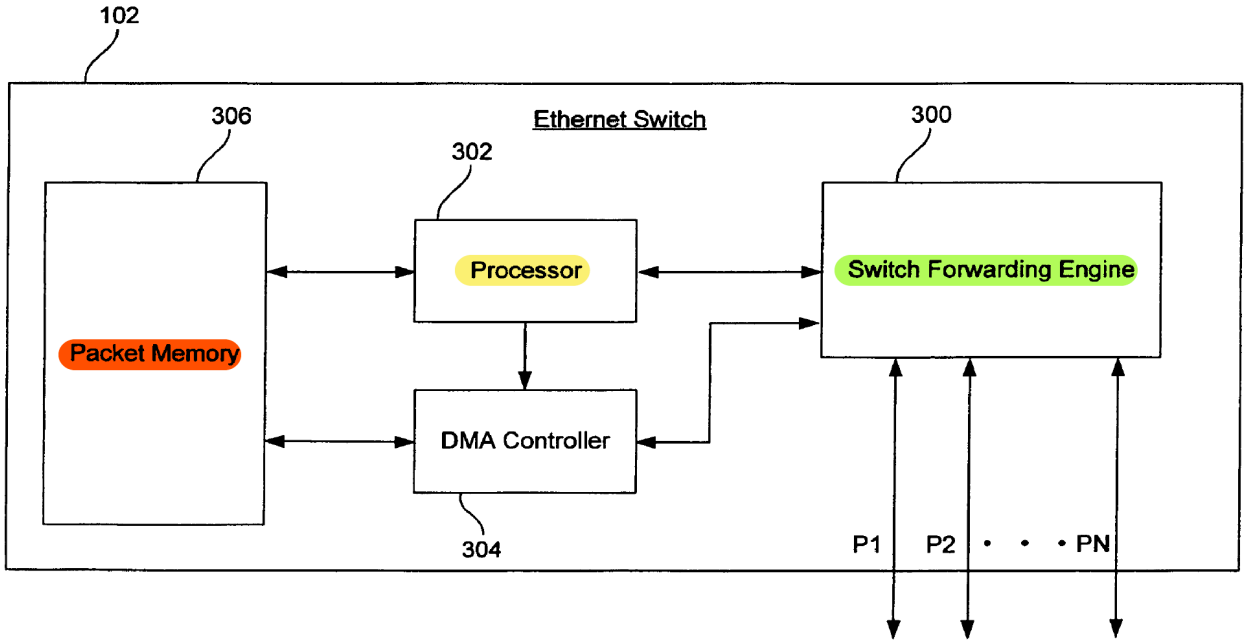


FIG. 3

Ex. 1001, Fig. 3 (annotated).

49. The red Packet Memory 306 corresponds to the claimed "memory circuit," the yellow Processor 302 corresponds to the claimed "processor," and the

green Switch Forwarding Engine 300 corresponds to the claimed "forwarding circuit."

VII. WHY THE CHALLENGED CLAIMS ARE NOT INVALID.

A. A POSITA Would Not Have Been Motivated To Combine The Gai, Yip and/or Kwan References On April 8, 2004.

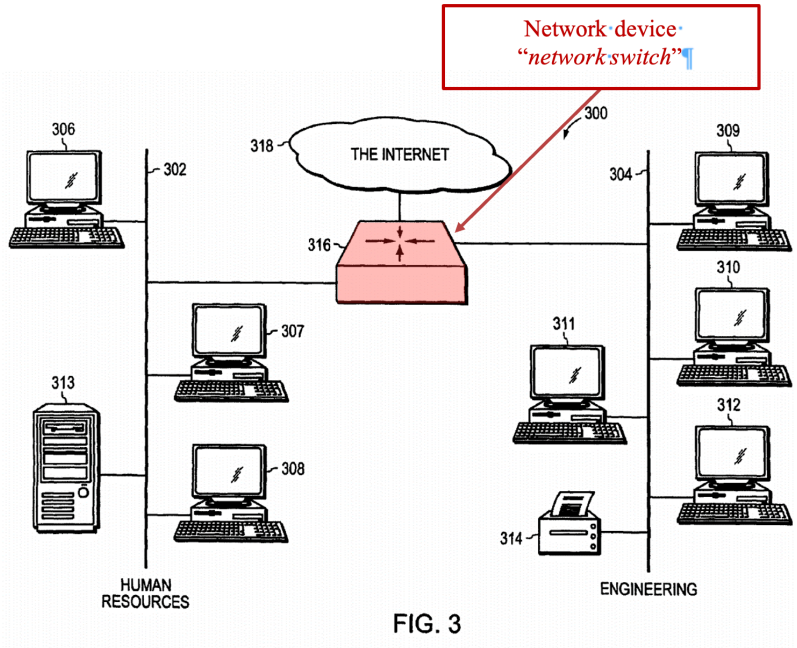
50. For the limitations of claims 1 and 3, the Petition and Dr. Crovella rely on three references. The first reference is U.S. Patent No. 6,651,096 to Gai et al. (Ex. 1006, "Gai") and is entitled "Method and Apparatus for Organizing, Storing and Evaluating Access Control Lists." The second reference is U.S. Patent No. 8,751,647 to Yip et al. (Ex.1013, "Yip") and is entitled "Method and Apparatus for Network Login Authorization." The third reference is U.S. Patent No. 7,523,485 to Kwan (Ex.1007, "Kwan") and is entitled "System and Method for Source IP Anti-Spoofing Security." *See* Petition at 9-42; Ex. 1003, ¶¶ 35-132.

51. A POSITA would have considered these references in the context of the layers of the Open Systems Interconnection (OSI) Reference Model and especially Layer 2, the data link layer, Layer 3, the network layer, and Layer 4, the transport layer.

52. In Gai, "[t]he invention relates to a method and apparatus for efficiently organizing, storing and evaluating access control lists (ACLs) for use by an ***intermediate network device*** of a computer network." Ex. 1006, Abstract (emphasis

Lionra Technologies Ltd.
Ex. 2001 - Page 23

added). A POSITA would have understood that Gai is directed to and discloses a Layer 3 intermediate device. "***Preferably, intermediate network device 316 is a layer 3 intermediate device and thus operates up to the network layer of the communication protocol stack implemented within the network 300***. For example, device 316 preferably includes an Internet Protocol (IP) software layer. Device 316 may also implement network services such as route processing, path determination and path switching functions. In the illustrated embodiment, device 316 is a computer having transmitting and receiving circuitry and components, including network interface cards (NICs), establishing physical ports and interfaces for exchanging network messages." Ex. 1006, 5:23-36 (emphasis added).



Ex.1006, Fig. 3 (annotated).

Petition, 33.

53. Although Gai discusses Layer 2 devices, a POSITA would have understood that Gai's disclosure was directed to Layer 3 switching devices. "[I]ntermediate devices, commonly referred to as routers, may operate at higher communication layers, such as layer 3, which in TCP/IP networks corresponds to the Internet Protocol (IP) layer. IP message packets include a corresponding header which contains an IP source address and an IP destination address. Routers or layer 3 switches may re-assemble or convert received data frames from one LAN standard (e.g., Ethernet) to another (e.g. Token Ring). Thus, layer 3 devices are often used to interconnect dissimilar subnetworks. Some layer 3 intermediate network devices may also examine the transport layer headers of received messages to identify the corresponding TCP or UDP port numbers being utilized by the corresponding network entities. Such extended-capability devices are often referred to as Layer 4, Layer 5, Layer 6, Layer 7 switches or Network Appliances." Ex. 1006, 2:9-24.

54. As taught by Gai, "[t]he term layer 3 intermediate device as used [in Gai] are intended broadly to cover any intermediate device operating primarily at the internetwork layer, including, without limitation, routers as defined by Request for Comments (RFC) 1812 from the Internet Engineering Task Force (IETF), intermediate devices that are only partially compliant with RFC 1812, intermediate devices that provide additional functionality, such as Virtual Local Area Network

(VLAN) support, IEEE 802.1Q support and/or IEEE 802.1D support, etc." *Id.*, 5:35-44. Gai's boilerplate recitation of possible applicability to "switches and/or layer 2 intermediate devices" would have been considered by a POSITA in the context of Gai's detailed disclosure of a Layer 3 device and its assertion that it could "operate with other, possibly far more complex, network topologies." *Id.*, 5:44-59. A POSITA would not have considered a Layer 2 device to be a more complex network topology. *See also* Ex. 1006, 62-65 ("A suitable platform for intermediate network device 316 are the Catalyst 8500® series of switch routers and/or the Catalyst® 6000 family of multi layer switches both from Cisco Systems, Inc.").

55. A POSITA would also have understood that the Access Control Lists discussed in Gai were directed to Layer 3 switching. *See, e.g.*, *Id.*, 16:63-17:25 (discussing, e.g., Source and Destination Port Identification, Internet Protocol Source and Destination Address Fields).

56. Gai's primary goal is to achieve higher switching speeds. As Gai teaches, "[t]here is no need for the forwarding entity 404 to evaluate multiple ACLs for each message. In addition, the evaluation of the single, unified ACL is performed by the TCAM ***at much higher speeds***. Accordingly, forwarding entity 404 can ***process messages much more quickly than the prior art devices***. In addition, ACL evaluation through the TCAM 410 preferably takes place in hardware rather than

software. That is, forwarding entity 404 may include one or more Application Specific Integrated Circuits (ASICs) for extracting and supplying the relevant information to TCAM 410, unlike the prior art devices in which ACL evaluation is performed by one or more software modules or libraries. ***The present invention is thus able to achieve much higher switching speeds than the prior art devices***. ***Indeed, the forwarding entity 404 of the present invention is effectively able to process network messages at rates of multi-Gigabits per second.***" Ex. 1006, 17:51-67.

57. The second reference is U.S. Patent No. 8,751,647 to Yip et al. (Ex.1013, "Yip") and is entitled "Method and Apparatus for Network Login Authorization."

58. Yip is directed to completely blocking access to a port until a lengthy authorization process is completed. Yip teaches "control[ing] the admission of a user to a network by preventing a port through which the user connects to the network from forwarding data packets until the user is authorized. A network login controller operates in conjunction with a user interface to receive a user identification data from the port user. The network login controller further operates in conjunction with an authorization server to authenticate the user by sending a user authentication request containing the user identification data to the authentication

Lionra Technologies Ltd.
Ex. 2001 - Page 27

server. The network login controller grants or denies permission to the user to access the network based on the user authentication response from the authentication server. If permission is granted, then the network login controller unblocks the port through which the user is connected to place it in packet-forwarding mode." Ex. 1013, Abstract.

59. Yip teaches assigning temporary IP addresses, which is inconsistent with Gai's Access Control Lists. In Yip, "prior to obtaining the user identification data 121, the end station/host computer H11 211 needs at least a temporary IP address to gain access to the network login controller 110 and associated user interface 120 on packet-forwarding device 200." *Id.*, 7:66-8:3. In Yip, "[s]ometimes, the end station/host computer needs to obtain a temporary IP address from the packet-forwarding device 200 before network login authorization 100 can take place, such as in the case of a campus environment where a roaming user will not always be using the same port for authentication. In one embodiment, assigning a temporary IP address to end station/host computer H11 211 is handled by an IP address server 130." *Id.*, 8:8-16. Yip further teaches that "[i]n one embodiment, at processing block 405 of FIG. 5, the user connects to a port of a packet-forwarding device 200 and, if necessary, obtains a temporary IP address from an IP address server 130 accessible to device 200. In one embodiment, the IP address server 130

is a DHCP server that may reside on the network 300, or in the packet switching device 200 itself. A temporary IP address is required in the campus environment where a typical user is a roaming user that may connect to the network from any number of ports that are available at various locations on the campus." *Id.*, 9:21-30.

60. Yip only discusses using a MAC address in alternate embodiments. "In an **alternate** embodiment, a static layer-2 address, such as the user's end station MAC address may be adequate for purposes of obtaining access to the network login controller 110 and user interface 120 on packet-forwarding device 200." *Id.*, 6:23-28 (emphasis added). "In some cases the end station/host computer, e.g. H11 211, uses its MAC address, …" *Id.*, 8:3-4. However, Yip does not explain when or why or how a MAC address would be used, and a POSITA would not consider Yip's bare assertion that a MAC address could be used, without more, as teaching the use of MAC addresses.

61. Moreover, Yip teaches blocking a specific port. A POSITA would not look to Yip's teaching of blocking a port until a lengthy authentication process had been completed in connection with Gai's teaching of high-speed network switching. Blocking one or more ports for an indeterminate time would be antithetical to Gai's goal of higher switching speeds and faster processing of messages.

62. In the Declaration of Dr. Mark E. Crovella Under 37 C.F.R. § 1.68 In Support of Petition for *Inter Partes* Review (Ex. 1003, "Declaration"), Dr. Crovella argues that a POSITA "would have been motivated to combine the teachings of Yip with Gai", as both are "analogous art to the '518 patent" through their shared field of computer networks and focus on similar problems such as using access control lists. Dr. Crovella provides a brief description of the functionality for Gai by stating "device 316 utilizes text-based access control list with various criteria initially set up by an administrator for processing packets", as well as arguing that "It was generally known in the art for ACLs to include MAC addresses to provide additional security and functionality, such allowing only devices with known addresses to communicate on the network". *See* Ex. 1003, ¶¶ 51-55.

63. Dr. Crovella then states that, as "[c]onsistent with general knowledge in the art, Yip teaches that it was known in the art for an administrator to include MAC addresses in ACLs," citing Ex. 1013, 2:43-47, which explains the purpose of access lists to combat "cyber-attacks on the LAN switch by providing an administrator-controlled list of Internet Protocol (IP) addresses or media access control (MAC) addresses that were authorized to access the network." *See* Ex. 1013, 2:43-47. Dr. Crovella then claims that this combination of Yip and Gai would have been obvious to a POSITA when creating one or more text-based ACLs, to include

MAC addresses of devices authorized to access the network. *See* Ex. 1003, ¶¶ 56-57.

64. I do not agree with Dr. Crovella's assertions that it would have been obvious for a POSITA to combine the text-based ACLs to include MAC addresses of devices authorized to access the network, nor would there be a motivation to combine the technologies as indicated by Dr. Crovella. During the relevant time frame, April 2004, network systems were often viewed as and divided into multiple layers throughout the industry. MAC addresses, which were typically used only for granular hardware level device management within a local area network (LAN) were usually hosted in the data link layer of the network, while ACLs were hosted in the Network and transport layers. Crossing these layers would lead to inefficiencies and increase network complexity, leading to potential new vulnerabilities and higher costs for implementation. Dr. Crovella does not address the inherent incompatibility and complexity a combination of Yip and Gai would introduce into a network and does not explain how a combination would be done in an effective manner other than his assertions that a combination would in theory work together at the time. The separation of the layers went against general industry understanding at the time, and presented more problems than the end result could justify. This combination would not have been viewed as a feasible option from a network professional's standpoint

in April 2004 and would have been avoided as a potential performance killer and costly endeavor for any company that attempted to implement it. A POSITA would not think to combine ACLs and MAC addresses due to their inherent separation within network layers causing complexity and performance issues when theoretically combined. The '518 Patent illustrates a novel invention concept that could feasibly bridge these separate functions in a way that would not decrease performance and introduce unnecessary network complexity to a network system.

65. The third reference is U.S. Patent No. 7,523,485 to Kwan (Ex.1007, "Kwan") and is entitled "System and Method for Source IP Anti-Spoofing Security."

66. A POSITA would understand that Kwan's teachings are directed to the subnet or Layer 2 level. "One approach to improving defenses against Source IP Spoofing is to attack the problem at the subnet or Layer 2 level." Ex. 1007, 3:21-23.

67. Kwan discloses a Layer 2 device. "FIG. 2 shows a view of an embodiment of a network device 200 of the present invention. This network device provides layer 2 switching functions." *Id.*, 3:42-45. "The network device 200 contains a processing device which operates to analyze data, packets received on a port to identify the MAC address of the host sending the data packet. Each data packet can include at least the MAC address of the device sending the data packet

Lionra Technologies Ltd.
Ex. 2001 - Page 32

(source MAC address) and the MAC address of the device to which the data packet is to be sent to (destination MAC address)." *Id.*, 3:59-64.

68. Although Kwan recognizes that "each host on the subnet can also have an IP address," *id.*, 3:67, a POSITA would understand that Kwan's teachings are directed to a subnet with limited connectivity. A POSITA would understand this because Kwan contemplates limiting each port to a single host, *id.,* 6:30-31 ("If there is more than one host device allowed per port, …") and teaches limiting the number of IP addresses associated with each port. "Additional MAC address and IP address pairs will continue to be learned until the maximum number of MAC and IP Addresses is reached." 6:36-38. *See also Id.*, 6:60-7:5.

69. Kwan also teaches a lengthy and time-consuming process for learning the correct IP address. "[A] tiered, or delayed, approach is required to successfully detect the source IP address. This approach could allow for first identifying the MAC address and then waiting for an appropriate amount of time to learn the correct IP address." *Id.*, 6:5-8. "It is also advantageous to confirm that the learned IP address is correct by performing a reverse IP check." *Id.*, 6:25-27.

70. A POSITA would not be motivated to combine Kwan's teachings of a subnetwork Layer 2 device with Gai's teachings of a Layer 3 intermediate device because a POSITA would recognize that what works for Layer 2 switching generally

does not apply to Layer 3 switching. A POSITA would also recognize that limiting the number of hosts that can connect to a single port or requiring a lengthy process for learning the correct IP address as taught by Kwan would be contrary to Gai's stated goal of achieving higher switching speeds.

71. In his Declaration, Dr. Crovella claims that it is obvious to combine the alleged prior art Gai and Kwan references because they are allegedly analogous art and the purported benefits a theoretical combination could produce. Dr. Crovella highlights that "In the circumstance of a dynamically assigned IP address, a POSITA would have recognized that it would be beneficial to learn a new IP address so that the network device 316 applies the latest data when processing packets," thus applying updated security rules appropriate for "the device to which the IP address was assigned." Ex. 1003, ¶ 66. Dr. Crovella asserts that Kwan meets this theoretical added functionality, as it "discloses a network device 200 that provides switching functions…" and "uses an ACL that is formatted for content addressable memory" including "source IP address and [a] corresponding MAC address [that are] correlated with each other as a source IP address/MAC address pair", with the pair used to control access and switch ports. Ex. 1003, ¶¶ 67-68. Dr. Crovella then focuses on a specific configuration of Kwan that scans for new IP addresses. *Id.*, ¶ 68.

72. I do not agree with Dr. Crovella's assertions that a POSITA would have found it obvious to implement Gai's administrator text-based ACLs to include MAC addresses as well as seed IP addresses and learn IP addresses, nor do I agree that there would be a motivation to combine the technologies as indicated by Crovella. For the same reasons articulated in my analysis of Dr. Crovella's reasons to combine the Gai and Yip references, it would not be obvious to a POSITA nor viewed as feasible to combine the functionality of ACLs and MAC addresses, a requirement necessary for a combination of Gai and Kwan to function as stated. Adding another layer of functionality, mapping dynamic IP addresses to MAC addresses within a text-based ACL function further increases the complexity and resources required, which would lead to performance issues and high cost for implementation.

73. In addition, adding dynamic IP learning functionality to ACLs including MAC addresses would introduce new vulnerabilities into the network, such as IP spoofing the MAC address into applying incorrect security controls. Dr. Crovella argues that this combination of technology provides additional security by "reducing false learning" and "combating source IP spoofing," but ignores the conceptual hurdle that adding to the amount of network components relying on an updated dynamic IP address could result in more reliance on faulty information. During the relevant time period, a network security POSITA would have viewed a

combination of IP address properties and MAC addresses in text-based ACLs as far too complex and vulnerable to integrate into a network with the certainty needed for network security.

74. For these reasons, I disagree with the Petition and Dr. Crovella that a POSITA would have been motivated to combine the Gai, Yip and Kwan references to satisfy the limitations of claims 1 and 3 of the Challenged Patent.

B. A POSITA Would Not Have Been Motivated To Combine The Gai, Yip, Kwan and Georgiou References On April 8, 2004.

75. For the limitations of claims 15, 17, and 19-21 of the Challenged Patent, the Petition and Dr. Crovella rely on the Gai Patent (as modified per Yip and Kwan) and U.S. Patent No, 7,003,597 to Georgiou et al. ("Georgiou"). *See* Petition at 9, 43-85; Ex. 1003, ¶¶ 133-257.

76. Independent claim 15 recites limitations to a dynamic access control list, specifically [15.1.5] subject to access restrictions contained in a dynamic access control list; [15.2.4] [the memory circuit…operable to store]…a dynamic access control list; [15.3.3] [the processor…] operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list and; [15.3.4] [the processor…operable to…] store the dynamic access control list in the memory circuit.

77. The Petition and Dr. Crovella assert that these "dynamic access control list" limitations would have been obvious to a POSITA who would have been motivated to combine Gai, Yip and Kwan. *See* Petition at 63-65, 69, 73-76; Ex. 1003, ¶¶ 180-187, 201-204, 214-221.

78. Independent claim 19 recites limitations to a dynamic access control list, specifically [19.1.6] subject to access restrictions contained in a dynamic access control list; [19.2.4] [the memory circuit…operable to store]…a dynamic access control list; [19.3.3] operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list and [19.3.4] [the processor… operable to…] store the dynamic access control list in the memory circuit.

79. The Petition and Dr. Crovella assert that these "dynamic access control list" limitations would have been obvious to a POSITA who would have been motivated to combine Gai, Yip and Kwan. *See* Petition at 80-81; Ex. 1003, ¶¶ 236, 240, 243-244.

80. For the reasons stated above with respect to challenged claim 1, I disagree with the Petition and Dr. Crovella that a POSITA would have been motivated to combine the Gai, Yip, Kwan and Georgiou references to satisfy the

dynamic access control list limitations of independent claims 15 and 19 of the Challenged Patent.

81. Claims 17, 20 and 21 are dependent claims that incorporate the limitations of the independent claims, including the dynamic access control list limitations, and I disagree with the Petition and Dr. Crovella that a POSITA would have been motivated to combine the Gai, Yip, Kwan and Georgiou references to satisfy the dynamic access control list limitations incorporated by reference in dependent claims 17, 20 and 21 for the same reasons stated above with respect to challenged claim 1.

82. In his Declaration, Dr. Crovella argues that it would have been obvious to combine the teachings of Gai and Georgiou. Dr. Crovella highlights a technological limitation in Gai where the process of forwarding a significant number of packets for processing in the CPU would create processing delays as the packet flow outpaces the processing capabilities. Dr. Crovella offers Georgiou as a solution to this issue, based on Georgiou's purported teaching of a process of storing packets temporarily in dynamic memory until the CPU is freed up based on Georgiou's statements regarding "receiv[ing] and temporarily stor[ing] the incoming packets in a memory … until subsequent processing can access and retrieve the packets, as appropriate, for action on the packet contents." Ex. 1003, ¶¶ 138-139. Dr. Crovella

states that this combination would "make more efficient use of Gai's network bandwidth." *Id.*, ¶ 141.

83. I do not agree with Dr, Crovella's arguments that a POSITA would find it obvious to combine the alleged teachings of Georgiou and Gai as described. Firstly, a POSITA considering a hypothetical combination of Georgiou and Gai as described would instantly note that the reliance on dynamic memory to store packets would bottleneck the system greatly within a relatively fast time frame as packets fill up the dynamic memory and slow down the stream of data to a crawl during filtering processes. Temporary storage in dynamic memory would lead to further network inefficiencies as the flow of packets would still outpace processing capabilities, meaning that there would be a net increase in the overall number of packets over time, regardless of how many packets can be redirected to dynamic memory. Further, implementing this process would be extremely costly and inefficient, as well as conceptually incompatible with the typical methods of switch hardware to forward packets at the highest sustainable rate as designed. A POSITA would thus view a combination of switch hardware storing packets and storing packets in the CPU as an unrealistic and impractical goal to implement in the network.

84. I disagree with Dr. Crovella's assertions that a POSITA would view a combination of Kwan, Yip, Gai, or Georgiou as an obvious combination because of the inherent separation of MAC addresses and ACL lists, the introduction of massive performance issues, and increased vulnerability within a system that would be too complex, costly, and incompatible for a realistic integration.

C. The Non-Volatile Random Access Memory (NVRAM) 408, Dynamic Memory 409, and TCAM 410 Disclosed in Gai Do Not Meet the Limitation of a "Memory Circuit Coupled to the Forwarding Circuit" recited in claims 15 and 19.

85. For the limitations of claims 15, 17, and 19-21, the Petition and Dr. Crovella rely on the Gai Patent (as modified per Yip and Kwan) and U.S. Patent No, 7,003,597 to Georgiou et al. ("Georgiou"). *See* Petition at 9, 43-85; Ex. 1003, ¶¶ 133-257.

86. Independent claim 15 recites limitations to a memory circuit, specifically [15.2.1] a memory circuit coupled to the forwarding circuit; [15.2.2] the memory circuit operable to store packets; [15.2.3] [the memory circuit…operable to store]…an enhanced access control list; [15.2.4] [the memory circuit…operable to store]…a dynamic access control list; [15.3.1] a processor coupled to the forwarding circuit and to the memory circuit; [15.3.3] [the processor…] operable to process the specific packets stored in the memory circuit using the enhanced access control list

to generate the dynamic access control list; and [15.3.4] [the processor…operable to…] store the dynamic access control list in the memory circuit.

87. The Petition and Dr. Crovella assert that the claimed "memory circuit" limitation of claim 15 is disclosed by the non-volatile random access memory (NVRAM) 408, dynamic memory 409, TCAM 410 and memory 411 in Gai as modified by Yip, Kwan, and Georgiou. *See* Petition at 65-71, 73-76; Ex. 1003, ¶¶ 188-208, 214-221.

88. Independent claim 19 recites limitations to a memory circuit, specifically [19.2.1] a memory circuit coupled to the forwarding circuit; [19.2.2] the memory circuit operable to store packets; [19.2.3] [the memory circuit…operable to store]…an enhanced access control list; [19.2.4] [the memory circuit…operable to store]…a dynamic access control list; [19.3.1] a processor coupled to the forwarding circuit and to the memory circuit; [19.3.3] [the processor…] operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list; and [19.3.4] [the processor…operable to…] store the dynamic access control list in the memory circuit.

89. The Petition and Dr. Crovella assert that the claimed "memory circuit" limitation of claim 19 is also disclosed by the non-volatile random access memory (NVRAM) 408, dynamic memory 409, TCAM 410 and memory 411 in Gai as

modified by Yip, Kwan, and Georgiou. *See* Petition at 80-81; Ex. 1003, ¶¶ 237-240, 241, 243-244.

90. The Petition and Dr. Crovella identify four separate circuits in Gai as corresponding to "a memory circuit" in independent claims 15 and 19 of the Challenged Patent. *See* Petition at 65-71, 73-76; 80-81; Ex. 1003, ¶¶ 188-208, 214-221, 237-240, 241, 243-244.

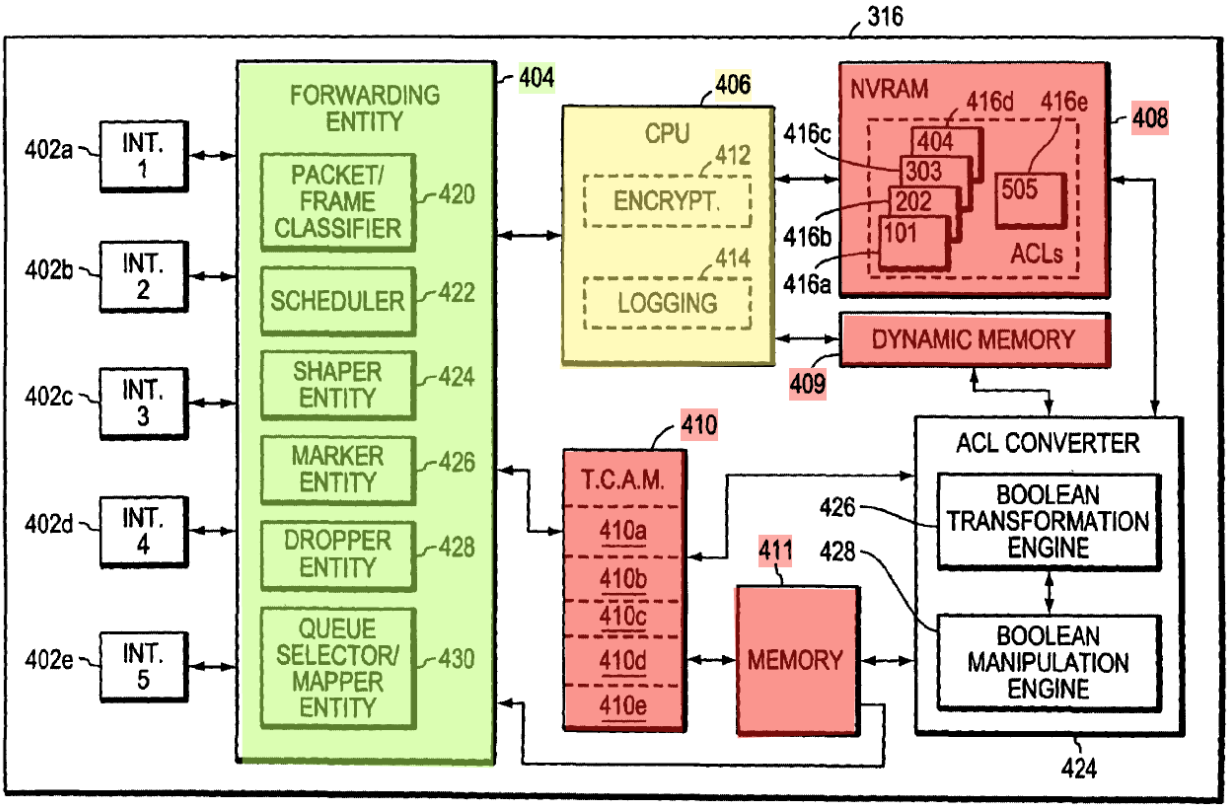


FIG. 4

Ex. 1006, Fig. 4 (annotated with yellow processor, green forwarding circuit and red memory circuit(s)).

91. In Gai, "[d]evice 316 further includes at least one forwarding entity 404, a central processing unit (CPU) 406, non-volatile random access memory (NVRAM) 408, dynamic memory 409 and at least one content addressable or associative memory 410. The associative memory 410 is preferably a ternary content addressable memory (TCAM), and its cells (not shown) may be associated with or assigned one of three values, such as "0", "1" or "don't care". Associated with and coupled to the TCAM 410 is another memory device 411, such as a dynamic random access memory." *Id.*, 5:66-6:9.

92. A POSITA would ***not*** have understand that four different memory circuits (or devices) correspond to a single memory circuit as recited in claims 15 and 19 of the Challenged Patent. A POSITA would have recognized that the different types of memory in Gai – non-volatile RAM, dynamic memory, and content addressable memory – could not be combined into a single memory circuit operable to store packets, enhanced control lists, and dynamic control lists.

93. A POSITA would also have understood that Gai's four different memory circuits (or devices), along with a fifth memory circuit or device to store packets, would not correspond to a single memory circuit as recited in claims 15 and 19 of the Challenged Patent as Petitioner and Dr. Crovella suggest. *See* Petition, 43-47; Ex. 1003, ¶¶ 133-144.

94. A POSITA would have recognized that storing Internet Protocol (IP) packets in memory as allegedly taught by Georgiou would be incompatible with Gai's goal of higher switching speeds and faster processing of messages. As Gai teaches, "[t]here is no need for the forwarding entity 404 to evaluate multiple ACLs for each message. In addition, the evaluation of the single, unified ACL is performed by the TCAM ***at much higher speeds***. Accordingly, forwarding entity 404 can ***process messages much more quickly than the prior art devices***. In addition, ACL evaluation through the TCAM 410 preferably takes place in hardware rather than software. That is, forwarding entity 404 may include one or more Application Specific Integrated Circuits (ASICs) for extracting and supplying the relevant information to TCAM 410, unlike the prior art devices in which ACL evaluation is performed by one or more software modules or libraries. ***The present invention is thus able to achieve much higher switching speeds than the prior art devices***. ***Indeed, the forwarding entity 404 of the present invention is effectively able to process network messages at rates of multi-Gigabits per second.***" Ex. 1006, 17:51-67.

95. Gai teaches that "the processing and forwarding of packets by the network device is substantially improved" because "[w]ith a single, unified ACL defined per interface per direction and stored in a CAM-type memory, the

intermediate network device is able to rapidly evaluate network messages. In particular, upon receipt of a packet at a first interface, a forwarding entity at the intermediate network device tests the packet against the single, unified ACL stored in the corresponding portion of the CAM. When a match is obtained, the corresponding decision is returned to the forwarding entity, which then takes the appropriate action (e.g., forward, discard, log and forward, transfer to CPU for additional processing, etc.) Since the intermediate network device only evaluates a single, unified ACL stored in the CAM, rather than multiple ACLs stored in RAM, a decision can be rapidly obtained." *Id.*, 4:26-42.

96. Georgiou has a diametrically opposite approach. In Georgiou, "after reception of a packet from the network interface, the packet is typically temporarily stored in an inbound buffer in the network interface from where it is then transferred to memory to await subsequent processing." Ex. 1013, 3:18-22.

97. A POSITA would not have been motivated to combine Gai and Georgiou's teachings because any modification to Gai in accordance with Georgiou's teachings would have **slowed** Gai's processing and been directly contrary to Gai's goal of faster processing, as well as adding increased complexity (e.g., a DMA circuit).

98. A POSITA would have recognized that Gai teaches that the processor is coupled to NVRAM 208 and dynamic memory 409. "CPU 406, …, is coupled to NVRAM 408, which may contain one or more text-based access control lists (ACLs) 416*a*-416*e*, such as ACLs 101, 202, 303, 404 and 505, and also to dynamic memory 409." *Id.*, 6:13-18. A POSITA would have recognized that NVRAM 408 and dynamic memory 409 are not "a memory circuit … operable to store packets and operable to store … a dynamic access control list" as claimed. A POSITA would understand that transient packets would not be stored in non-volatile RAM (NVRAM).

99. A POSITA would also have recognized that Gai teaches that "[t]he forwarding entity 404 is also coupled to the CPU 406, the TCAM 410, which may be apportioned into segments 410*a*-*e* whereby each segment 410*a*-*e* corresponds to a particular interface 402*a*-*e*, and memory 411." *Id.*, 6:23-28. A POSITA would have recognized that TCAM 410 and memory 411 are not "a memory circuit … operable to store packets and operable to store an enhanced access control list" as claimed. A POSITA would understand that transient packets would not be stored in ternary content addressable memory (TCAM).

100. A POSITA would have further recognized that Gai's teachings include "an access control list (ACL) converter 424 [that] is operatively coupled to NVRAM

408 for accessing the text-based ACLs 416*a-e*, dynamic memory 409 for processing the ACLs 416*a-e*, and to TCAM 410 and its associated memory 411 for storing modified versions of the ACLs 416*a-e* …" *Id.*, 6:36-41. A POSITA would have recognized that an ACL converter does not correspond to either the claimed processor or forwarding circuit as identified by the Petition and Dr. Crovella, and would therefore not couple the memory to either the processor or the forwarding circuit.

101. A POSITA would have also recognized that Gai does not disclose or teach a memory circuit operable to store packets. In Gai, "[t]he message [packet] 100 is captured and provided to the forwarding entity 404." *Id.*, 16: 67-17:1. In Gai, "the forwarding entity 404 is basically configured to forward or switch network messages among the various interfaces 402*a-e* of device 316." *Id.*, 6:27-31. Even if a POSITA would have considered adding an additional DMA circuit operable to store packets, as suggested by a combination of Gai and Georgiou as proposed by the Petition and Dr. Crovella, which a POSITA would not have done for at least the reasons stated above, that resulting quintet of circuits would not have corresponded to "a memory circuit" as claimed in claims 15 and 19 of the Challenged Patent.

102. For these reasons, I disagree with the Petition and Dr. Crovella that the non-volatile random access memory (NVRAM) 408, dynamic memory 409, TCAM

410, and memory 411 in Gai teach, suggest, or disclose the "memory circuit" limitations of claims 15 and 19 of the Challenged Patent.

103. For these reasons, I also disagree with the Petition and Dr. Crovella that a POSITA would have understood from the combined teachings of Gai and Georgiou that Gai and Georgiou teach, suggest or disclose the "memory circuit" limitations of claims 15 and 19 of the Challenged Patent.

104. Claims 17, 20 and 21 are dependent claims that incorporate the limitations of the independent claims, including the memory circuit limitations, and I disagree with the Petition and Dr. Crovella that the combined teachings of Gai and Georgiou or the non-volatile random access memory (NVRAM) 408, dynamic memory 409 and TCAM 410 in Gai disclose, teach or suggest the "memory circuit" limitations incorporated by reference in dependent claims 17, 20 and 21 for the same reasons stated above with respect to challenged claims 15 and 19.

I 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 that these statements were made with knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, undersection 1001 of Title

18 of the United States Code.

Date: January 22, 2025



Dr. Eric Cole

APPENDIX – LISTING OF CHALLENGED CLAIMS AND EXHIBITS

[1.0]. A method of developing an access control list, comprising:

[1.1] developing an enhanced access control list including data related to at least one of user names, DNS names, Windows domain names, and physical addresses;

[1.2.1] converting, in a network switch, at least one of:

[1.2.2] user names into corresponding IP and physical addresses according to data in the enhanced access control list, wherein converting user names into corresponding IP and physical addresses according to data in the enhanced access control list includes:
detecting login packets being communicated over the network;
determining a MAC address from the login packets;
detecting server message block login packets being communicated over the network;
determining an IP address from the server message block login packets; and
developing records in the access control list using the obtained IP address for the respective user name;

[1.2.3] DNS names into corresponding IP addresses according to data in the enhanced access control list; and

[1.2.4] physical addresses into IP addresses according to data in the enhanced access control list; and

[1.3] developing, in the network switch, the access control list from each of the operations of converting.

[3.1] The method of claim 1 wherein each physical address comprises a MAC address.

[15.0] A network switching circuit, comprising:

[15.1.1] a forwarding circuit operable to detect specific received packets and

[15.1.2] to provide the specific packets on a processor port, and

[15.1.3] further operable to receive packets on one of a plurality of ports including the processor port

[15.1.4] and to forward each received packet to a port corresponding to a destination address contained in the packet

[15.1.5] subject to access restrictions contained in a dynamic access control list;

[15.2.1] a memory circuit coupled to the forwarding circuit,

[15.2.2] the memory circuit operable to store packets and

[15.2.3] operable to store an enhanced access control list and

[15.2.4] a dynamic access control list; and

[15.3.1] a processor coupled to the forwarding circuit and to the memory circuit,

[15.3.2] the processor operable to define the specific packets detected by the forwarding circuit and

[15.3.3] operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list and

[15.3.4] store the dynamic access control list in the memory circuit, and

[15.3.5] further operable to provide the specific packets to the processor port of the forwarding circuit after processing the packets.

[17.1] The network switch of claim 15 wherein the switch comprises an Ethernet switch and wherein the packets comprise Ethernet packets.

[19.0] A computer network, comprising:

[19.1.1] a network switch, including,

[19.1.2] a forwarding circuit operable to detect specific received packets and

[19.1.3] to provide the specific packets on a processor port, and

[19.1.4] further operable to receive packets on one of a plurality of ports including the processor port and

[19.1.5] to forward each received packet to a port corresponding to a destination address contained in the packet

[19.1.6] subject to access restrictions contained in a dynamic access control list;

[19.2.1] a memory circuit coupled to the forwarding circuit,

[19.2.2] the memory circuit operable to store packets and

[19.2.3]operable to store an enhanced access control list and

[19.2.4]a dynamic access control list; and

[19.3.1] a processor coupled to the forwarding circuit and to the memory circuit,

[19.3.2] the processor operable to define the specific packets detected by the forwarding circuit and

[19.3.3] operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list and

[19.3.4] store the dynamic access control list in the memory circuit, and

[19.3.5] further operable to provide the specific packets to the processor port of the forwarding circuit after processing the packets; and

[19.4] a plurality of hosts, each host coupled to a respective port of the network switch.

[20.1] The computer network of claim 19 wherein at least some of the hosts comprise personal computer systems.

Ex.1001	U.S. 7,623,518
Ex.1002	Prosecution History of U.S. 7,623,518
Ex.1003	Declaration of Mark E. Crovella, Ph.D. under 37 C.F.R. § 1.68
Ex.1004	*Curriculum Vitae* of Mark E. Crovella, Ph.D.
Ex.1005	Complaint filed on May 9, 2024
Ex.1006	U.S. Patent No. 6,651,096 to Gai et al. ("Gai")
Ex.1007	U.S. Patent No. 7,523,485 to Kwan ("Kwan")
Ex.1008	U.S. Patent No. 7,003,597 to Georgiou et al. ("Georgiou")
Ex.1009	U.S. Patent No. 6,105,086
Ex.1010	U.S. Patent Publication No. 2001/0012294A1
Ex.1011	U.S. Patent No. 5,720,032
Ex.1012	U.S. Patent No. 5,797,033
Ex.1013	U.S. Patent No. 8,751,647
Ex.1014	U.S. Patent No. 7,343,485
Ex.1015	Median time-to-trial in the Eastern District of Texas
Ex.1016	U.S. Patent Publication No. 2005/0055570A1
Ex.1017	Intellinet User Manual
Ex.1018	Netgear WG602 Users Guide
Ex.1019	Email from Seth Hasenour to Emily Whitcher, "Re: Lionra vs. Cisco (Lionra II) – Letter," December 4, 2023.
Ex.1020	Docket Control Order, *Lionra Techs. Ltd. v. Cisco Systems, Inc.*, No. 2:23-cv-00206, Dkt. 30 (E.D. Tex. Aug. 9, 2023).
Ex. 2001	Declaration of Eric Cole in Support of Patent Owner's Response
Ex. 2002	*Curriculum Vitae* of Eric Cole