



CISCO SYSTEMS, INC. Petitioner,
V.
LIONRA TECHNOLOGIES LIMITED, Patent Owner

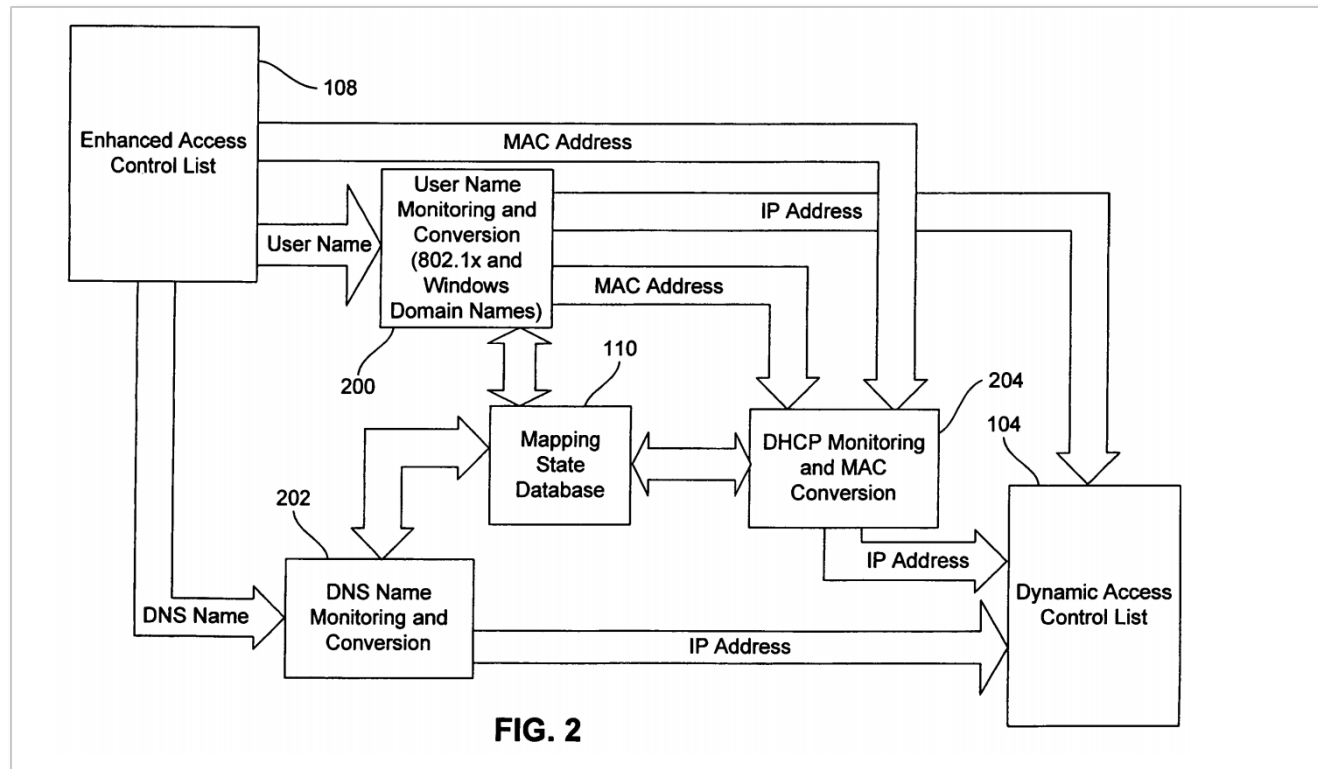
Case No. IPR2024-00734
U.S. Patent No. 7,623,518

Gregory P. Huh
Haynes and Boone, LLP

July 14, 2025



The '518 Patent



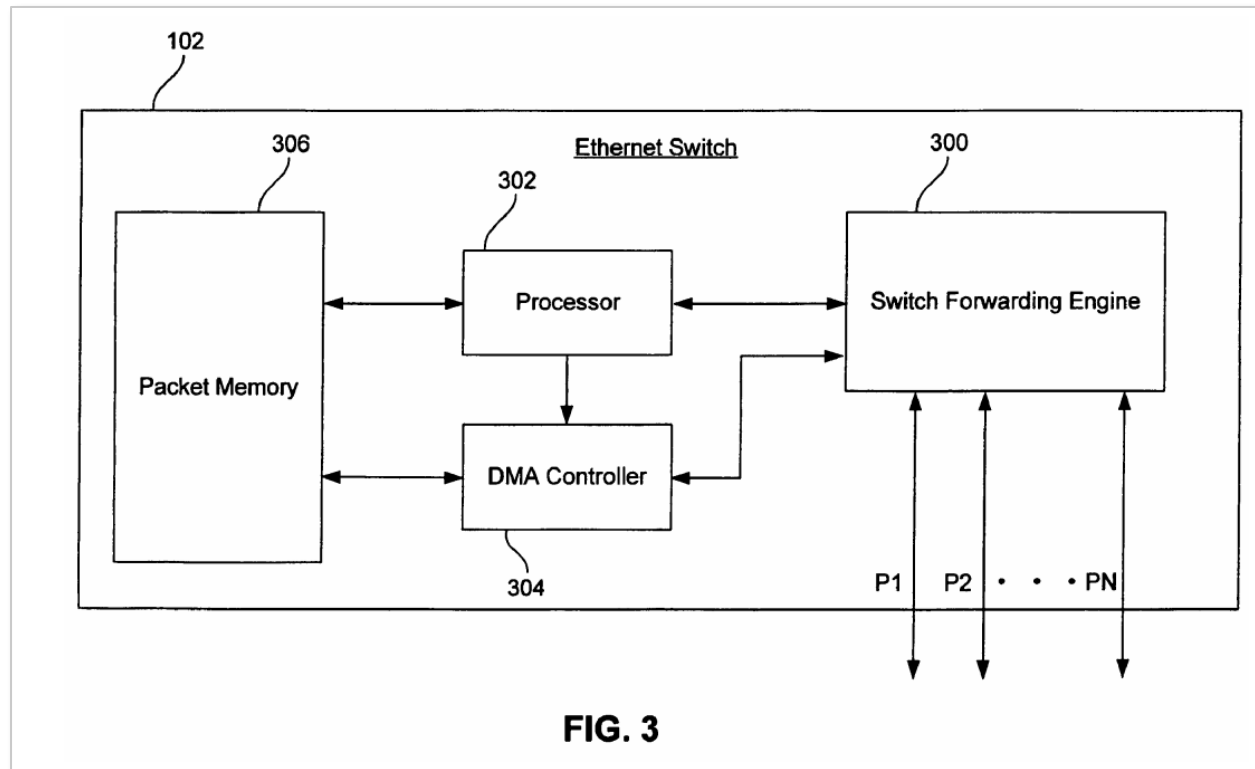
Ex.1001, Fig. 2.

1. A method of developing an access control list, comprising:

- developing an enhanced access control list including data related to at least one of user names, DNS names, Windows domain names, and physical addresses;
- converting, in a network switch, at least one of:
 - 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;
- DNS names into corresponding IP addresses according to data in the enhanced access control list; and
- physical addresses into IP addresses according to data in the enhanced access control list; and
- developing, in the network switch, the access control list from each of the operations of converting.

Ex.1001, Claim 1.

The '518 Patent



Ex.1001, Fig. 3.

15. A network switching circuit, comprising:
- a forwarding circuit operable to detect specific received packets and to provide the specific packets on a processor port, and further operable to receive packets on one of a plurality of ports including the processor port and to forward each received packet to a port corresponding to a destination address contained in the packet subject to access restrictions contained in a dynamic access control list;
 - a memory circuit coupled to the forwarding circuit, the memory circuit operable to store packets and operable to store an enhanced access control list and a dynamic access control list; and
 - a processor coupled to the forwarding circuit and to the memory circuit, the processor operable to define the specific packets detected by the forwarding circuit and 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 store the dynamic access control list in the memory circuit, and further operable to provide the specific packets to the processor port of the forwarding circuit after processing the packets.

Ex.1001, Claim 15.

Key Points

1. A POSITA would have been motivated to combine Gai and Yip
2. A POSITA would have been motivated to combine Gai and Kwan
3. A POSITA would have been motivated to combine Gai, Kwan, and Georgiou
4. The prior art teaches “*a memory circuit*” of claim 15

Gai's intermediate device is a multilayer switch that uses an access control list

Gai

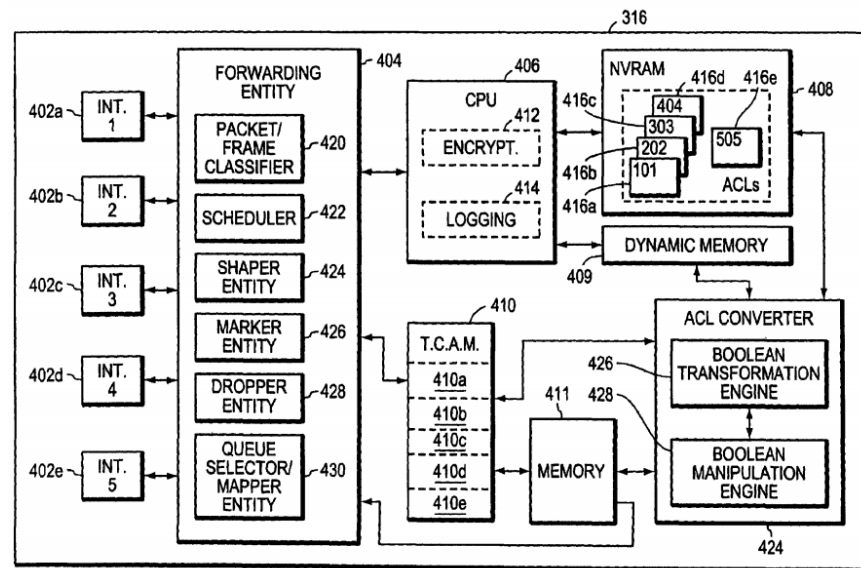


FIG. 4

Ex.1006 (Gai), FIG. 4; Petition, 11.

Gai

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. A suitable TCAM **410** for use with the

Ex.1006 (Gai), 6:62-65; Reply, 11, 15.

First, a network administrator creates one or more access control lists in a conventional manner. For example, the administrator preferably utilizes a conventional text editor at a management station (not shown) to create the access control lists. FIGS. 5A-5E are highly schematic representations of text-based ACLs **416a-416e**, respectively. Each

Ex.1006 (Gai), 7:15-21; Petition, 25.

Yip teaches that it was known in the art for an access control list to include MAC addresses

Yip

For example, access lists were developed 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. DoS and SYN attack protections are

Ex.1013 (Yip), 2:43-47; Petition, 15, 26-27.

Yip's teachings would improve security in Gai because only specific MAC addresses would be permitted

Dr. Crovella

57. It would have been obvious to a POSITA for Gai's administrator, when creating one or more text-based ACLs, to include MAC addresses of devices authorized to access the network, per Yip. Including the MAC address in Gai's text-based ACLs would beneficially allow for dynamically generating TCAM ACLs with MAC addresses to thereby restrict or permit access based on MAC address. Such an implementation would improve security because only specific MAC addresses would be permitted to communicate packets over the network. Adding the additional feature of being able to filter packets based on MAC addresses is consistent with Gai's goal of providing security and implementing additional features with its ACLs. Ex.1006, 8:3-6.

Ex.1003 (Dr. Crovella Declaration), ¶57; Petition, 15-16.

Both experts agree that a POSITA would have known how to implement the combination with a reasonable expectation of success

Dr. Crovella

60. The reasonable expectation of success is also supported by others that had implemented ACLs with MAC addresses. *See e.g.,* Ex.1014, 6:30-32, 8:27-47, 11:57-62 (disclosing a table that includes IP/MAC addresses corresponding to an access control list); Ex.1017, 55 (“If you choose ‘Allowed Listed’, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When ‘Deny Listed’ is selected, these wireless clients on the list will not be able to connect to the Access Point.”); Ex.1018, 13 (“Access Control List... Click Allow or Block to enable MAC address filtering. Click Disable to disable Access Control feature...Enter the MAC address for each station to be managed, in the MAC Address field and click Add.”).

Ex.1003 (Dr. Crovella Declaration), ¶60; Petition, 16-17.

Dr. Cole

Q. Doctor, it was known in the art for a layer 2 network switch to have an access control list stored in CAM that includes both the IP address and the MAC address. Correct?

A. I believe I answered that several times. Kwan talks about an IP address and MAC address pair being stored in ACL CAM.

So, yes, Kwan talks about the IP address and MAC address being stored in ACL CAM.

Ex.1021 (Dr. Cole Deposition), 50:22-51:6; Reply, 14.

Patent Owner incorrectly argues that Gai is directed to Layer 3 switching

Patent Owner Response

A POSITA would also have understood that the Access Control Lists discussed in Gai were directed to Layer 3 switching. *See, e.g.*, Ex. 1006, 16:63-17:25 (discussing, e.g., Source and Destination Port Identification, Internet Protocol Source and Destination Address Fields). Ex. 2001, ¶ 55.

Patent Owner Response, 11.

Gai

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

...

support, etc. Nonetheless, it should be understood that the present invention may also be utilized in whole or in part with other intermediate network devices, such as switches and/or layer 2 intermediate devices, which are also intended

Ex.1006 (Gai), 5:22-47; Patent Owner Response, 10; Reply, 6.

Patent Owner's expert conceded that Gai's intermediate network device is not limited to Layer 3

Dr. Cole

Q. So in that first part that you had just read, Gai states that the invention may be utilized in layer 2 intermediate devices. Correct?

A. It says that.

Ex.1021 (Dr. Cole Deposition), 109:10-13; Reply, 7.

Patent Owner's expert ignored Gai's disclosure

“[A] reference constitutes prior art for all that it teaches.”

In re Riggs, Case No. 2022-1945 (Fed. Cir. Mar. 24, 2025); Reply, 7.

Dr. Cole

Q. And you believe Gai is lying about that?

ATTORNEY AUCHTER: Objection to form.

A. No. But I believe if you look at the claims of Gai, it's referring to layer 3.

Q. So you're limiting your understanding of Gai to what it claims. Is that correct?

ATTORNEY AUCHTER: Objection to form.

A. I mean, to me, the claims are the invention. So the specification could talk about sort of hypotheticals and things like that. But to me, the invention is what's in the claims.

Ex.1021 (Dr. Cole Deposition), 109:14-21; Reply, 7.

Gai's intermediate network device may be implemented with a Cisco 6000 multi layer switch

Gai

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. A suitable TCAM **410** for use with the

Ex.1006 (Gai), 6:62-65; Reply, 11, 15.

Both experts agree that Cisco's multi layer switch 6000 operates at Layer 2

Dr. Crovella

9. A POSITA would have understood that Cisco's Catalyst® 6000 multilayer switch is configurable to operate at multiple layers, including operating at Layer 2 to perform ACL filtering, as illustrated below at Figure 7.5:

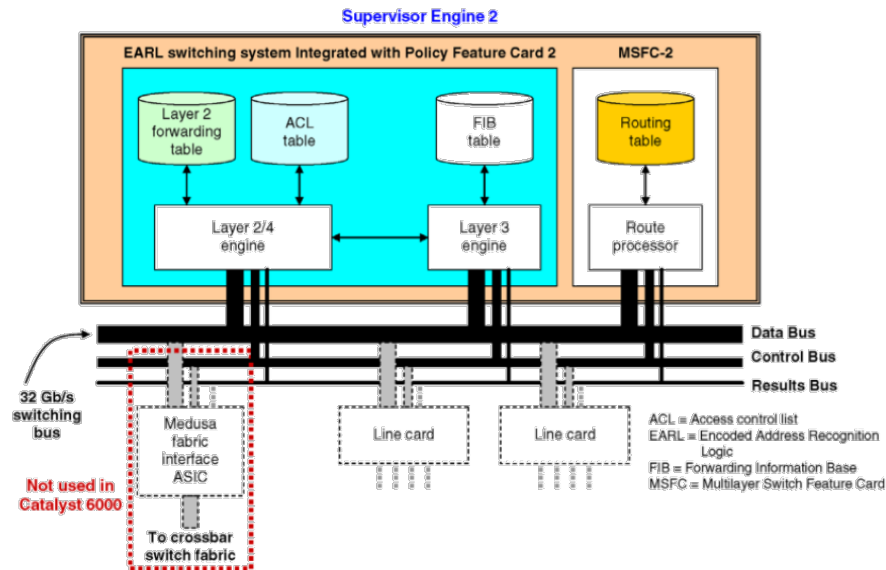


FIGURE 7.5 Catalyst 6000 with Supervisor Engine 2 with Policy Feature Card 2 (PFC2) and Multilayer Switch Feature Card 2 (MSFC2).

Dr. Cole

So when you're saying multilayer switches, it means it's operating on layers 2 and 3,

Ex.1021 (Dr. Cole Deposition), 111:18-19; Reply, 11.

Ex.1023 (Dr. Crovella Declaration), ¶9; Reply, 10.

Patent Owner Sur-Reply untimely new argument is improper

“A sur-reply may only respond to arguments raised in the corresponding reply.”

37 C.F.R. § 42.23(b); *Google LLC v. Uniloc 2017 LLC*, IPR2020-00447, Paper 24 at 13–14 (PTAB May 11, 2021).

Patent Owner Sur-Reply

In fact, Yip teaches away from using MAC addresses, which are machine or hardware based.

Patent Owner Sur-Reply, 7.

Patent Owner Sur-Reply argues for the first time that “Yip teaches away from using MAC addresses,” which was never argued in the Response.

Key Points

1. A POSITA would have been motivated to combine Gai and Yip
2. A POSITA would have been motivated to combine Gai and Kwan
3. A POSITA would have been motivated to combine Gai, Kwan, and Georgiou
4. The prior art teaches “*a memory circuit*” of claim 15

Kwan teaches how to learn new IP addresses based on MAC addresses in an access control list

Kwan

attached to the port. To determine if the data packets received at a port contain a new source IP address that has not been learned, the ACL-CAM compares the source IP address and the MAC address in a received data packet, with the table of IP address/MAC address pairs.

...

The source IP address detector 236, can learn the source IP address for a host in a number of different ways. For example, the source IP address can be learned by using a reverse address resolution protocol (RARP) which provides for sending out the MAC address on the subnet, and in response the host having the MAC address responds with its IP address. The source IP address detector 236 could also learn the IP address for a host by listening to the DHCP response packet being returned to the host. This response contains the source IP Address for the host. When a DHCP packet is detected, the entry in the table for the MAC address receiving the DHCP packet with a source IP address is cleared and the source IP address provided in the DHCP packet is loaded into the table.

Ex.1007 (Kwan), 5:25-50; Petition, 19, 52.

Learning DHCP IP addresses based on MAC addresses provides numerous benefits

Dr. Crovella

address properties in the text-based ACLs, Gai's network device 316 would be able to process packets from a host that has a known MAC address but has been assigned a new IP address (e.g., using DHCP), as was often done at the time.

Ex.1007, 1:66-2:1 ("The IP address is often assigned using the Dynamic Host Configuration Protocol (DHCP)"). Such an implementation would obviate the need for Gai's administrator to manually generate updated text-based ACLs when the network changes. Ex.1006, 2:57-60, 4:6-13, 7:16-20, 18:3-5; Ex.1007, 7:67-8:1.

Since a computer's MAC address is generally static, incorporating Kwan's use of a MAC address in Gai's ACLs would allow the administrator to specify access control rules that are applied to a specific computer irrespective of the IP address assigned dynamically to that computer.

Ex.1003 (Dr. Crovella Declaration), ¶70; Petition, 20.

Dr. Cole

So it's much more scalable and easier just to turn on DHCP, so this way every computer can get the same exact image. There's no -- there's no manual configuration there.

Ex.1021 (Dr. Cole Deposition), 36:22-25; Reply, 16.

Reasonable expectation of success in learning IP addresses using MAC addresses

Dr. Crovella

74. Also, a POSITA would have had a reasonable expectation of success in applying Kwan's IP address learning techniques (e.g., RARP and DHCP) based on the MAC addresses, since RARP and DHCP were standardized protocols and well known in the art. Ex.1011, 21:1-3; Ex.1014, 1:15-28; Ex.1017, 5; Ex.1018, 4. The reasonable expectation of success is also supported by the specific details that Kwan provides to learn new IP addresses based on MAC addresses using RARP and DHCP techniques.

Ex.1003 (Dr. Crovella Declaration), ¶74; Petition, 22.

Patent Owner's switching speeds and spoofing arguments are meritless

“Our caselaw is clear. It’s not necessary to show that a combination is ‘the *best* option, only that it be a *suitable* option.’”

Intel Corp. v. Qualcomm Inc., 21 F.4th 784, 797 (Fed. Cir. 2021)(citation omitted)(emphasis in original); Reply, 19.

Patent Owner Response

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. Ex. 2001, ¶ 70.

...

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. *Id.*, ¶ 73. Petitioner’s

Patent Owner Response, 18.

Patent Owner's arguments about switching speeds and spoofing are meritless

Dr. Crovella

14. I also disagree with Patent Owner and Dr. Cole that Kwan's teachings would adversely impact Gai's switching speeds because the number of hosts are limited. Resp. 18; Ex.2001, ¶¶69-70. A POSITA would have understood that the switching speeds are not diminished if the number of hosts are limited per port—there is no logical relationship. Gai obtains high switching speeds by utilizing ACL TCAM. A POSITA would have recognized that Kwan's technique to learn a new IP address (e.g., one that was assigned with DHCP) does not impact switching speeds of an already learned IP addresses. In fact, Kwan's technique would benefit Gai because a new IP address would be learned quickly without manual administrator intervention, which is time intensive.

Ex.1023 (Dr. Crovella Declaration), ¶14; Reply, 18.

Dr. Crovella

teaches doing just that. Also, I disagree with the assertion that the proposed combination would introduce new vulnerabilities into the network, such as IP spoofing the MAC address. Resp. 18; Ex.2001, ¶¶72-73. To the contrary, a POSITA would have understood that in the combination vulnerabilities are reduced and IP spoofing the MAC address would not be an issue. In the proposed combination of Kwan with Gai (as modified per Yip), the MAC addresses are provided by the administrator as text inputs in the ACL and Kwan teaches that a seed IP address is provided by the administrator (*see* Ex.1007, 6:14-18). This means that spoofing in the combined system is reduced because an IP address attempting to spoof the MAC address would have to both spoof the IP (to match the seed) and the MAC address (to match a paired MAC address *see* Ex.1007, 3:1-4; 6:14-18), which would be very difficult.

Ex.1023 (Dr. Crovella Declaration), ¶15; Reply, 19.

Key Points

1. A POSITA would have been motivated to combine Gai and Yip
2. A POSITA would have been motivated to combine Gai and Kwan
3. A POSITA would have been motivated to combine Gai, Kwan, and Georgiou
4. The prior art teaches “*a memory circuit*” of claim 15

Gai teaches that certain packets are forwarded to the CPU for additional processing

Gai

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

Ex.1006 (Gai), 4:29-36; Petition, 54.

column 1008 corresponds to a NAT ACL. Another column 1010 presents the merged action to be implemented by the forwarding entity in response to the actions specified by the ACL features of columns 1002–1008. The final or merged actions to be implemented by a given forwarding entity may include permit, deny, forward to CPU for additional processing (e.g., encryption, logging, etc.), forward to an alternative forwarding entity, etc. The conflict resolution table

Ex.1006 (Gai), 13:38-45; Petition, 23, 45, 51.

Georgiou teaches using a DMA controller to store packets that need additional processing

Georgiou

Typical arrangements include employing some form of logic, either hardware centric or software centric, to receive and temporarily store the incoming packets in a memory area, e.g., a buffer pool or equivalent, until subsequent processing can access and retrieve the packets, as appropriate, for action on the packet contents. These arrangements may also employ distributed processing or centralized processing.

Ex.1008 (Georgiou), 1:22-29; Petition, 45.

its intended destination. The hardware attached to the input port is often a simple DMA circuit that receives the packet, writes it to memory, and then indicates to the controlling processor that a packet has been received.

Ex.1006 (Gai), 1:54-57; Petition, 45.

Numerous reasons to use a DMA controller to store packets that need additional processing

Dr. Crovella

- [1] 140. It would have been obvious to a POSITA, in view of Georgiou, to implement Gai's network switch to store packets forwarded to a CPU for additional processing (e.g., encryption, logging, learning IP addresses, etc.) in its dynamic memory. Storing the packets in memory would allow the packets awaiting processing to be retained until the CPU is freed up, thereby facilitating processing of packets (e.g., encrypt, log, learn new IP address, etc.).
- [2] 141. Additionally, because the packets are stored in dynamic memory, the packets are not dropped for lack of CPU processing bandwidth and can therefore be forwarded to the destination postprocessing. Ex.1007, 5:22-6:30; Ex.1008, 9:7-12.
- [3] The proposed combination would also reduce the number of packets that need to be retransmitted (since fewer packets would be dropped), and thus, make more efficient use of Gai's network bandwidth.

Ex.1003 (Dr. Crovella Declaration), ¶¶110-141; Petition, 46.

Reasonable expectation of success in using a DMA controller to store packets that need additional processing

Dr. Crovella

145. The results would have been predictable and there would have been a reasonable expectation of success in the combination given the similarity in Georgiou's and Gai's systems. Any modification needed to Gai, in order to accommodate the teachings of Georgiou, including implementing a DMA circuit to store incoming packets in Gai's dynamic memory, would have been a conventional and simple implementation and well within the level of one of ordinary skill in the art. Ex.1008, 1:54-57 ("...often a simple DMA circuit that receives the packet, writes it to memory, and then indicates to the controlling processor that a packet has been received."); Ex.1009, 1:32-34 ("A direct memory access (DMA) controller is often used."); Ex.1010, [0216], ("[M]essages can also be placed directly into CPU

Ex.1003 (Dr. Crovella Declaration), ¶145; Petition, 47.

Patent Owner's arguments about storing packets are meritless.

Dr. Crovella

17. Georgiou's teachings would not have slowed Gai's processing of incoming packets because in Gai, most packets are forwarded by Gai's forwarding entity 404 to their destination and only packets that Gai does not forward, e.g., because they need additional processing (e.g., encrypt, learn new IP addresses...) would be stored in dynamic memory 409. Ex.1006, 1:22-27, 5:44-67, 17:44-48. As such, in the proposed combination only a small number of packets (e.g., packets that need additional processing by CPU 406) are stored in the dynamic memory 409 and the majority of packets are forwarded by the forwarding entity 404 to the various interfaces 402a-e of device 316. Furthermore, the proposed combination would not be "extremely costly and inefficient" because using a DMA circuit and dynamic memory, as Georgiou teaches, was well known in the art and such well known devices would add minimal complexity to Gai's system that already has dynamic memory 409. Resp. 25; Ex.2001, ¶83.

Ex.1023 (Dr. Crovella Declaration), ¶17; Reply, 20-22.

Key Points

1. A POSITA would have been motivated to combine Gai and Yip
2. A POSITA would have been motivated to combine Gai and Kwan
3. A POSITA would have been motivated to combine Gai, Kwan, and Georgiou
4. The prior art teaches “*a memory circuit*” of claim 15

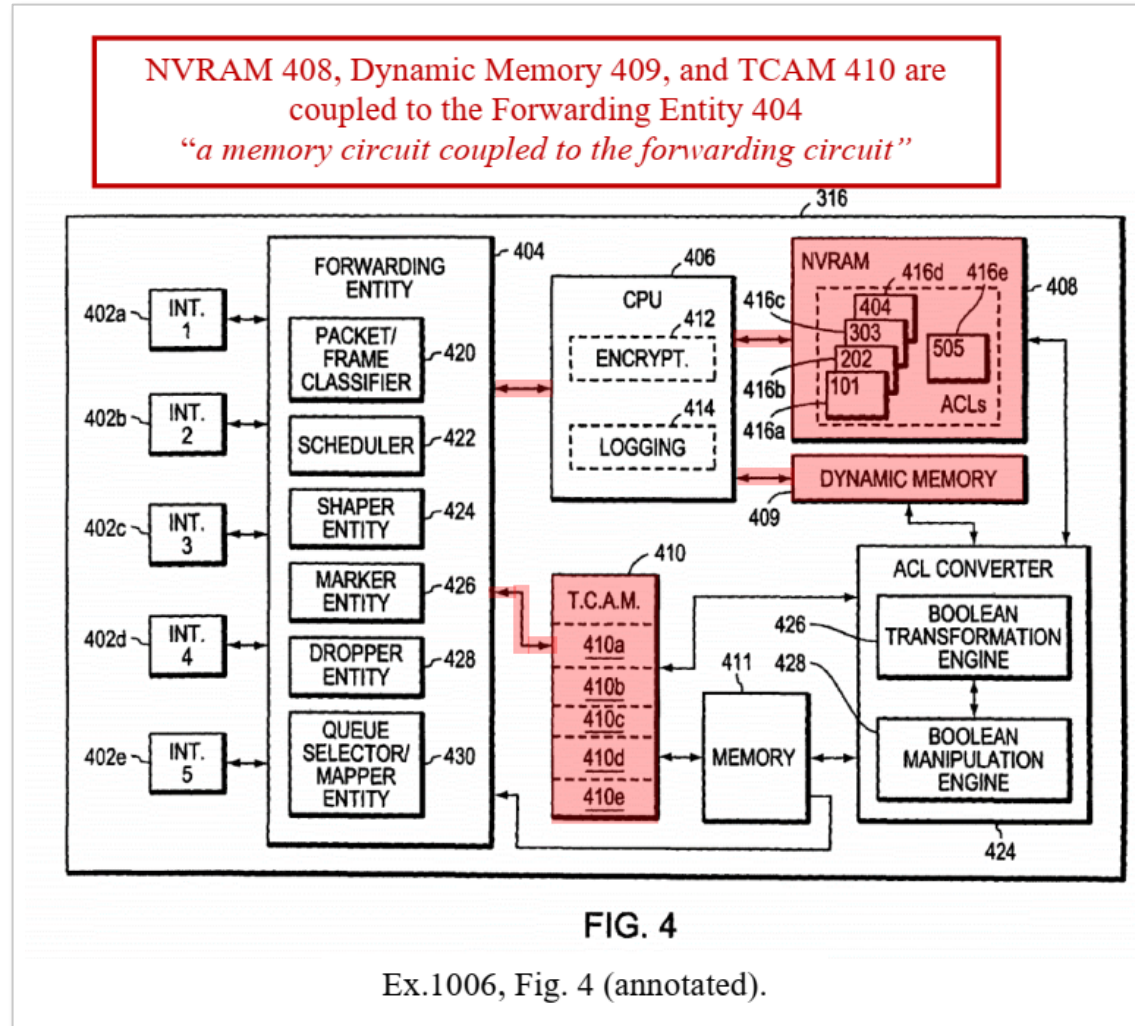
The '518 Patent

15. A network switching circuit, comprising:
a forwarding circuit operable to detect specific received packets and to provide the specific packets on a processor port, and further operable to receive packets on one of a plurality of ports including the processor port and to forward each received packet to a port corresponding to a destination address contained in the packet subject to access restrictions contained in a dynamic access control list;
a memory circuit coupled to the forwarding circuit, the memory circuit operable to store packets and operable to store an enhanced access control list and a dynamic access control list; and
a processor coupled to the forwarding circuit and to the memory circuit, the processor operable to define the specific packets detected by the forwarding circuit and 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 store the dynamic access control list in the memory circuit, and further operable to provide the specific packets to the processor port of the forwarding circuit after processing the packets.

Ex.1001, Claim 15.

Gai teaches “a memory circuit...”

Petition



Petition, 29; Reply, 21.

Patent Owner's implicit construction of “*a memory circuit...*” is meritless

“[T]he use of ‘a’ or ‘an’ in an open-ended ‘comprising’ claim connotes ‘one or more.’”

Celgene Corp. v. Peter, 931 F.3d 1342, 1350 (Fed. Cir. 2019); Reply, 24.

Patent Owner Response

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. Ex. 2001, ¶ 92.

Patent Owner Response, 30.

Patent Owner Sur-Reply

The written description in the '518 Patent is directed to a single memory circuit. As are the limitations of independent claims 15 and 19 which clearly recite a memory circuit coupled to a forwarding circuit and a processor wherein the packets and the enhanced and dynamic control lists are explicitly recited as being stored in the memory circuit.

Patent Owner Sur-Reply, 17.

Patent Owner's implicit construction is unsupported by the '518 specification

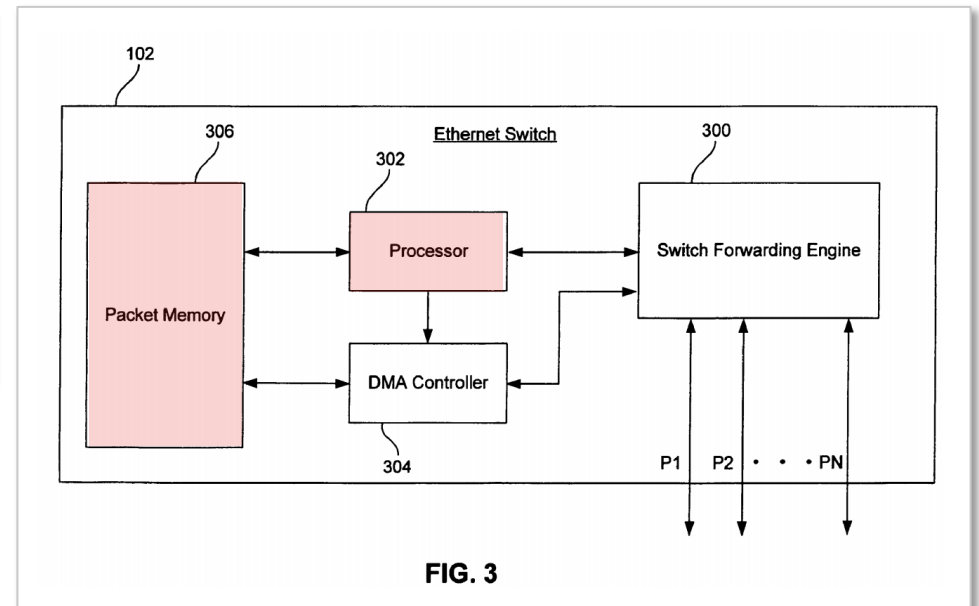
“a memory circuit...operable to store [1] packets and operable to store an [2] enhanced access control list and a [3] dynamic access control list.”

'518 Patent

The selected packets are stored in the packet memory 306 for processing by the processor 302. Also stored in either the packet memory 306 or memory in the processor 302 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

'518 patent, 9:28-36; Reply, 24.

'518 Patent



'518 patent, Fig. 3; Patent Owner Sur-Reply, 24.

Both experts agree that Patent Owner's implicit construction is unsupported by the '518 specification

“a memory circuit...operable to store [1] packets and operable to store an [2] enhanced access control list and a [3] dynamic access control list.”

Dr. Crovella

18. Lastly, in view of the specification, a POSITA would not understand the claims of the '518 patent to require a “single” “memory circuit.” There is no such embodiment disclosed in the '518 patent and the claim language broadly covers one or more “memory circuits.” Resp. 30; Ex.2001, ¶92.

Ex.1023 (Dr. Crovella Declaration), ¶18; Reply, 24-25.

Dr. Cole

Q. But you cannot identify a single embodiment where it discloses a single memory circuit that stores received packets, an enhanced access control list, and a dynamic access control list. Correct?

...

So, no, I can't find a specific reference in the specification that has the exact claim, but that's not to be my understanding. The claim is the invention. The specification provides details.

So, no, the specification doesn't have the specifics of the claim, but in my understanding, that's not required. The claim speaks for itself.

Ex.1045 (Dr. Cole Deposition), 40:1-7; Reply, 25.



The bridge to possible

