

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ARISTA NETWORKS, INC.,
Petitioner,

v.

CISCO SYSTEMS, INC.,
Patent Owner.

Case IPR2016-00306
Patent 7,023,853 B1

Before, BRYAN F. MOORE, MIRIAM L. QUINN, and
MATTHEW R. CLEMENTS, *Administrative Patent Judges*.

QUINN, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

Arista Networks, Inc. (“Petitioner”) filed a Petition to institute *inter partes* review of claim 63 of U.S. Patent No. 7,023,853 B1 (“the ’853 patent”) pursuant to 35 U.S.C. § 311–319. Paper 1 (“Pet.”). Cisco Systems, Inc. (“Patent Owner”) filed a Preliminary Response. Paper 7 (“Prelim. Resp.”). Upon consideration of the Petition and the Preliminary Response, we instituted trial. Paper 8 (“Dec.”).

During trial, Patent Owner filed a Patent Owner Response (Paper 19, “PO Resp.”); and Petitioner filed a Reply (Paper 24, “Reply”). An oral hearing was held on March 7, 2017.¹

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a). For the reasons discussed herein, and in view of the record in this trial, we determine that Petitioner has not shown by a preponderance of the evidence that claim 63 of the ’853 patent is unpatentable.

I. BACKGROUND

A. RELATED MATTERS

Petitioner identifies the patent-at-issue as the subject matter of a district court action filed, on December 5, 2014, in the Northern District of California (Civ. No. 4:14-cv-5343-JSW). Pet. 1. The ’853 patent is also involved in an International Trade Commission Investigation, instituted on January 20, 2015 (No. 337-TA-945). *Id.*

The ’853 patent also has been the subject of multiple petitions for *inter partes* review filed by Petitioner. *Id.* The following proceedings have

¹ A transcript of the oral hearing is entered in the record as Paper 34 (“Tr.”).

been identified: IPR2015-00976 (“the ’976 IPR”), IPR2015-01050 (“the ’1050 IPR”), and IPR2016-00304. *Id.*; PO Notice, Paper 6.

B. INSTITUTED GROUNDS

We instituted *inter partes* review of claim 63 based on anticipation by Spinney² under 35 U.S.C. § 102. Dec. 21.

Petitioner supports its contentions of unpatentability with a declaration from Dr. H. Jonathan Chao. Ex. 1002 (“Chao Declaration”). Patent Owner supports its contentions with a declaration from Dr. Kevin Almeroth. Ex. 2015 (“Almeroth Declaration”).

C. THE ’853 PATENT (EX. 1001)

The ’853 patent is titled, “Access Control List Processing in Hardware,” and relates generally to a method for performing access control list processing in hardware using an associative memory. Ex. 1001, 1:5–8. Data packets transmitted between network devices can be restricted using a technique known as “access control.” *Id.* at 1:14–20. One access control technique is to use access control lists or “ACLs” to determine whether to permit or deny transmission of a packet to a particular destination. *Id.* at 1:23–25 (“[T]he ACL describes which selected source devices are permitted (and which denied) to send packets to which selected destination devices.”).

The Specification provides an example of a known ACL format, where each ACL includes “access control specifiers.” *Id.* at 1:26–27. These specifiers contain information to match with incoming packets, and then based on a match, specify a particular access result (e.g., whether

² U.S. Patent No. 5,414,704 (“Spinney”) (Ex. 1004).

transmission of a packet is “specifically permitted or specifically denied”).
Id. at 1:27–34. Figure 1 of the ’853 patent is reproduced below.

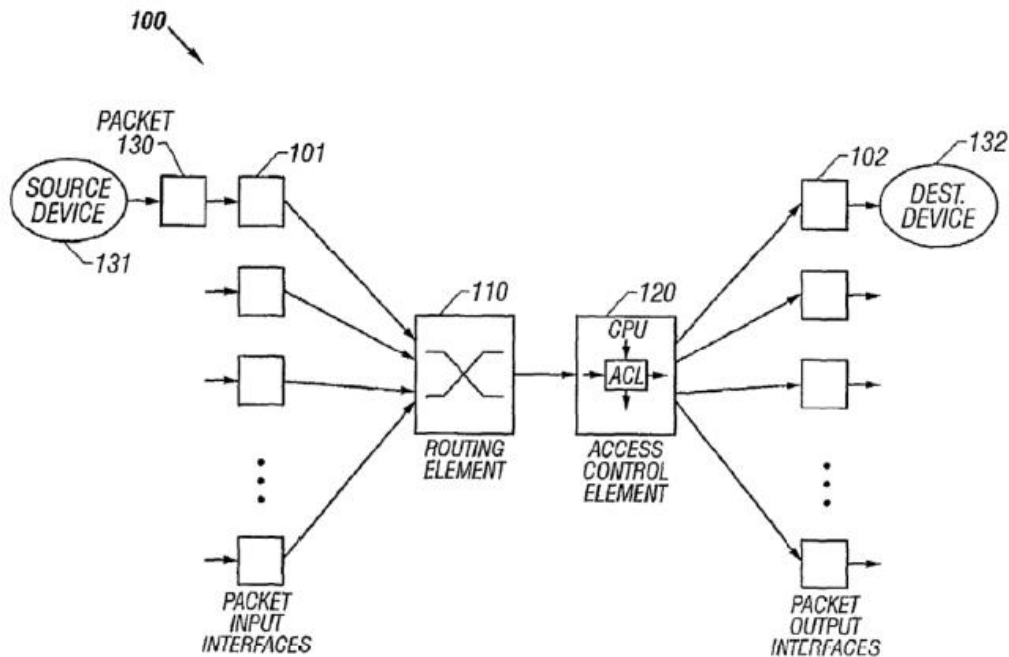


FIG. 1

Figure 1 is a block diagram of a system for performing access control in accordance with the ’853 patent. Ex. 1001, 3:22–23, 43–44. As shown in Figure 1, packet 130 arrives at one of the system’s packet interfaces 101. *Id.* at 3:47–48. Routing element 110 then selects one or more of the output interfaces to which the packet should be forwarded. *Id.* at 3:50–53. Prior to forwarding, access control element 120 determines whether to allow transmission of the packet. *Id.* at 3:53–57.

Figure 2 of the ’853 patent is reproduced below.

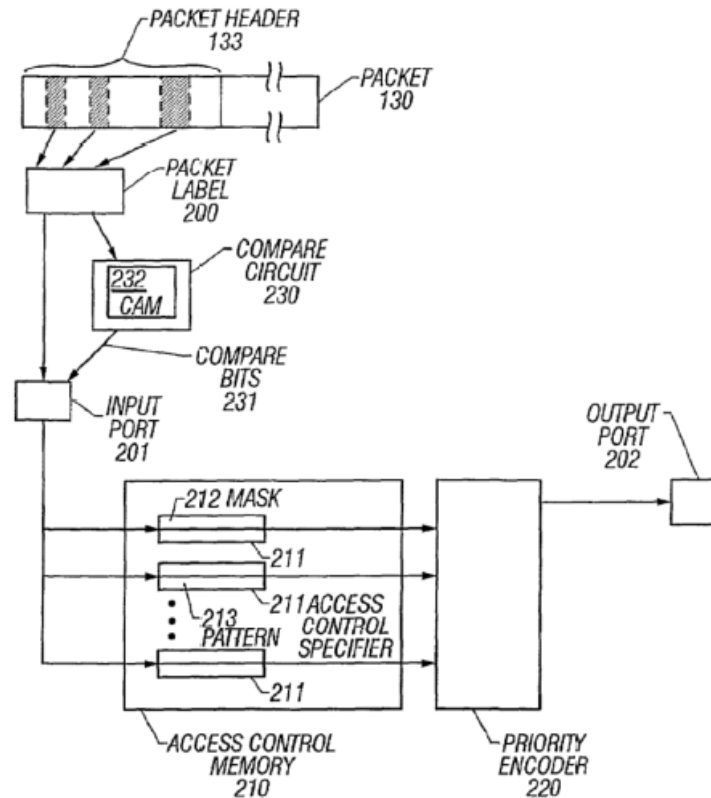


FIG. 2

Figure 2 is a block diagram of an access control element, which contains access control patterns. *Id.* at 4:17–18. When packet 130 arrives at access control element 120, packet label 200 is created based on information derived from packet header 133 of packet 130. *Id.* at 4:19–22. The information in packet label 200 is compared to label match mask 212 and label match pattern 213 of each access control specifier 211. *Id.* at 4:56–58. If a match is found with a particular access control pattern, priority encoder 200 selects the corresponding access control specifier 211 with the highest priority and provides an indicator of that access control specifier 211 to output port 202. *Id.* at 4:5–56, 5:10–14. The indicator specifies an access

control result, which specifies if the packet should be transmitted. *Id.* at 5:1–9.

D. CHALLENGED CLAIM

Challenged claim 63 is the only claim at issue in this proceeding.

63. A method of processing a packet comprising:
selecting an output interface to which to forward the packet;
determining forwarding permission for the packet, wherein the determining comprises matching one or more characteristics of said packet with one or more access control specifiers in at least one access control element;
processing said packet based on said forwarding permission;
wherein,
the selecting step is performed in parallel with the determining step.

II. ANALYSIS

A. CLAIM INTERPRETATION

In an *inter partes* review, claim terms in an unexpired patent are interpreted according to their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2142–46 (2016). Consistent with that standard, claim terms also are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). There are, however, two exceptions to that rule: “1) when a patentee sets out a definition and acts as his own

lexicographer,” and “2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution.” *See Thorner v. Sony Computer Entm’t Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

If an inventor acts as his or her own lexicographer, the definition must be set forth in the specification with reasonable clarity, deliberateness, and precision. *Renishaw PLC v. Marposs Societa’ per Azioni*, 158 F.3d 1243, 1249 (Fed. Cir. 1998) (citing *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994)). Although it is improper to read a limitation from the specification into the claims, *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993), claims still must be read in view of the specification of which they are a part, *Microsoft Corp. v. Multi-Tech Sys., Inc.*, 357 F.3d 1340, 1347 (Fed. Cir. 2004).

“access control specifiers”

In our Decision on Institution we preliminarily construed the phrase “access control specifiers” as “a specifier that includes information for matching with a packet and that may indicate, or aid in indicating, an access result.” Dec. 9–12. Neither party disputes this construction. *See* Pet. 6–7 (Petitioner stating that “for purposes of this proceeding, the broadest reasonable interpretation of the phrase ‘access control specifiers’ should” encompass the construction entered in the ITC proceeding); *see also* PO Resp. 14–15 (Patent Owner arguing that it relies on the Board’s construction of “access control specifier” as stated in the Decision on Institution). Accordingly, we adopt that construction in this proceeding.

“access control”

In our Decision on Institution we construed “access control” to mean “restriction on the transmission of a packet or alteration of a selected output

interface for the packet.” Dec. 6–9. In its Response, Patent Owner argues that the Board’s construction is overly broad and not consistent with the plain and ordinary meaning of the term. PO Resp. 7–14. Petitioner argues that Patent Owner’s arguments are irrelevant because claim 63 does not recite the term “access control.” Reply 19–20. We note that the term “access control” appears as part of two terms: “access control specifiers” and “access control element.” We have adopted an undisputed construction of the term “access control specifiers.” And there is no dispute regarding the scope of “access control element.” Accordingly, we agree with Petitioner that further analysis of the term “access control,” by itself, is unnecessary.

B. PRINCIPLES OF LAW

“[A] claim is anticipated if each and every limitation is found either expressly or inherently in a single prior art reference.” *King Pharm., Inc. v. Eon Labs, Inc.*, 616 F.3d 1267, 1274 (Fed. Cir. 2010) (quotations omitted). “In the context of anticipation, the question is not whether a prior art reference ‘suggests’ the claimed subject matter[;] . . . [r]ather, the dispositive question regarding anticipation is whether one skilled in the art would reasonably understand or infer from a prior art reference that every claim element is disclosed in that reference.” *AstraZeneca LP v. Apotex, Inc.*, 633 F.3d 1042, 1055 (Fed. Cir. 2010) (internal brackets and quotation marks omitted).

C. ANTICIPATION BASED ON SPINNEY

Petitioner alleges that claim 63 is anticipated by Spinney. Spinney is titled, “Address lookup in packet data communications link, using hashing and content-addressable memory.” Ex. 1004, [54]. Spinney relates to a way of doing source and destination address lookups in a packet data communication system, using a combination of hashing, binary search, and content-addressable memory (CAM) lookup. *Id.* at 1:34–38. Figure 1A of Spinney, reproduced below, depicts a block diagram of a controller that interfaces between an FDDI link and a crossbar switch.

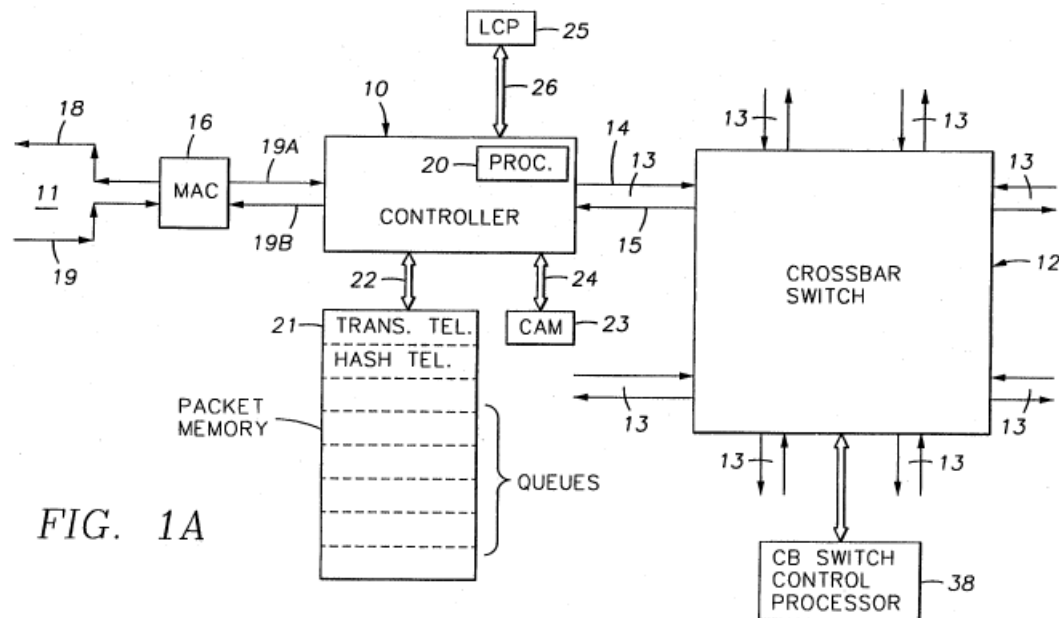


Figure 1A illustrates controller 10 containing a processor or state machine 20 to execute processes and access CAM 23 via interface 24. *Id.* at 5:45–49. Processor 20 executes two inbound packet-processing processes. *Id.* at 5:64–66. The processes can operate in parallel. *Id.* at 6:5–8. With respect to the first inbound process, inbound receive (IR), the processor receives packets, and the IR process parses and decodes each incoming packet. *Id.* at 6:17–21. The IR process determines if the packet is to be

forwarded to crossbar 12. *Id.* “For bridged packets, this decision is made by performing destination address, source address, and protocol field lookups, with the aid of the content addressable memory 23 and the internal hash function, according to the invention.” *Id.* at 6:21–25. The result of the lookup determines where the packet is to go. *Id.* at 6:25–26.

Spinney also describes that processor 20 in controller 10 performs functions related to inbound and outbound packets. *Id.* at 8:66–68. For example, Spinney describes that controller 10 “performs input port filtering to prevent undesired traffic from entering the net, and this filtering is based on certain addresses contained in a packet.” *Id.* at 9:3–6. “Certain addresses identified in the protocol as IEEE 802.2 LLC DSAP and IEEE 802.2 LLC SNAP can be filtered by checking against items stored in the CAM 23, e.g., 256 entries.” *Id.* at 9:9–12.

1. Operation of the CAM in Spinney

Much of the dispute between the parties hinges on the operation of the CAM in Spinney. Petitioner’s theory of unpatentability relies on Spinney’s CAM as disclosing the limitation of determining a forwarding permission for the packet (the “determining limitation”). Pet. 14. That theory also relies on Spinney’s use of a hash lookup as disclosing the limitation of selecting an output interface to which to forward the packet (the “selecting limitation”). *Id.* at 11. The claim requires that the selecting and determining limitations are performed in parallel. Thus, Petitioner argues that Spinney’s “hash lookup operation” and the “CAM lookup operation” are performed simultaneously. *Id.* at 16.

Patent Owner disputes Petitioner’s assertions regarding Spinney’s use of the CAM. According to Patent Owner, Petitioner has failed to show that

Spinney's CAM is used for determining forwarding permission. PO Resp. 29–30. Further, Patent Owner challenges Petitioner's assertions that Spinney filters based on the items in the CAM. *Id.* at 30–31. Patent Owner argues that Spinney, in sum, discloses using the CAM lookup for frame forwarding, but not for determining forwarding *permission* based on a match. *Id.* at 25–28.

We find that Spinney discloses various uses for its CAM. First, Spinney discloses using the CAM in combination with the hash lookup to solve the problem when more than one 48-bit address hashes to the same hash bucket. Ex. 1004, 3:23–27. In this scenario, the 48-bit address (the exact address) causing the collision is stored in the CAM. *Id.* at 3:25–27, 16:37–42. In this manner, if a 48-bit address does not cause a problem, the hash lookup will proceed to obtain the corresponding content of the translation table in the packet memory. *Id.* at 16:22–26. If there is a match for the 48-bit address in the CAM, the immediate result is an index to the translation table. *Id.* at 16:17–21.

Second, Spinney discloses that a CAM lookup, for the purpose for filtering, occurs for every address lookup. For example, Spinney describes that the use of the CAM to assist in the hash lookup process is without cost in time or new circuitry because every address is compared with the CAM entries anyways, to filter for multicast messages, SNAP filtering, etc. *Id.* at 16:42–45. Spinney describes that this CAM lookup is for every destination address. *Id.* at 16:16–19. Spinney also describes looking up in the CAM the special addresses in the logical link control (LLC) header. *Id.* at 9:9–12, 11:7–11. In particular, Spinney describes that arriving packets comprise

various headers, such as FDDI header 57, 802.2 LLC header 58, information field 59 (payload), and FDDI CRC field 60. *See id.* at Fig. 4, 10:66–11:2. The 802.2 LLC header includes certain addresses or information corresponding to specific protocols to be handled by a specific destination device or driver. *See* Ex. 2015 ¶¶ 110–112 (declarant explaining the purpose of DSAP and SNAP field extensions and their purpose in packet processing). It is this second, filtering operation of Spinney’s CAM that Petitioner relies on as disclosing the “determining limitation.” *See, e.g.*, Ex. 1002 ¶ 52 (Dr. Chao opining that Spinney’s disclosure of *filtering* by checking the CAM for these LLC addresses “confirms that the CAM lookup generally performs the task of determining if the packet has permission to be routed, though it also assists in the ‘small but finite’ set of problem conditions, with packet routing.”

2. *Whether Spinney Anticipates Claim 63*

The issue for us to decide is whether Spinney’s CAM lookup for filtering constitutes “determining forwarding permission for the packet” that is performed in parallel with Spinney’s hash lookup (the alleged “selecting step”). We find that Petitioner has not shown by a preponderance of the evidence that Spinney’s CAM lookup (alleged “determining” step) and hash lookup (alleged “selecting” step) are performed in parallel, as required by claim 63. Although the record is not entirely clear regarding how the CAM lookup aids in filtering, Spinney describes the IR process as the means to obtain the information necessary to construct the “gigaheader.” Ex. 1004, 11:38–48; *see also id.* at 6:32–35 (alluding to gigaheader). The gigaheader defines “how the packet is to be serviced” within the net and its processing is performed by examining the fields of this gigaheader. *Id.* at 11:44–47.

One of the fields of the gigaheader is the destination switch field, which identifies the switch number of the final destination of the packet within the net. *Id.* at 11:56–58. The purpose of the address lookup process using the hash lookup and the CAM lookup is to derive, at a minimum, this 12-bit destination switch value. *Id.* at 11:59–62; *see also* Ex. 1001, Appendix (cols. 17–18, 25–26) (setting forth the pseudocode for the FUNCTION AddressLookup, which returns the GigaAddressType that includes the 12-bit switchNumber value). One set of those values (00_{hex} and 01_{hex}) “indicate[s] that the final destination address is to be filtered at this port” and “[o]ther values derived for this field will direct the packet to its destination within the switch.” *Id.* at 11:68–12:3. Therefore, it is reasonable to infer from Spinney’s disclosure of filtering that the CAM lookup, if matching information in the LLC header, results in the IR process deriving the gigaheader for the packet. This gigaheader includes a destination switch value indicating that filtering will be performed at that port. This is consistent with the disclosure in column 9 of Spinney that describes handling the LLC header addresses as part of input port filtering. *Id.* at 9:3–12.

Although Spinney’s CAM lookup is part of the process of filtering the packet according to the LLC header, Spinney does not determine the filter information in parallel with the alleged “selecting” step in Spinney, i.e., the “forwarding lookup” according to Dr. Chao. *See* Ex. 1002 ¶ 53. Claim 63 recites “selecting an output interface to which to forward the packet.” Ex.1001, 12:21–22. We agree with Petitioner that Spinney discloses selecting an output interface using the hash lookup. *See* Pet. 11–12 (pointing to Spinney’s IR process including a hash lookup operation used to

determine the appropriate local address to be used in directing the packet to its destination). We also agree with Petitioner that Spinney discloses that the vast majority of address lookups are selected by the hashing function alone. *Id.* at 13 (citing Ex. 1001, 3:3–11). However, the only embodiment describing the interaction between the hash lookup (alleged “selecting” step) and the CAM lookup (alleged “determining” step), does not support Petitioner’s contention and Dr. Chao’s opinion that they are performed in parallel.

First, we give no credit to Dr. Chao’s opinion in this regard because it is not supported by Spinney. Specifically, we give no weight to Dr. Chao’s opinion that “Spinney makes clear that the CAM lookup and the hashing function (i.e., the forwarding lookup) take place at the same time.” Ex. 1002 ¶ 53. Instead, we find that the parallel operations in Spinney are confined to (1) applying the *hash function* to the 48-bit address and (2) performing a CAM lookup of the same 48-bit address. For example, Spinney discloses in Figure 8 that incoming address field 85 is subjected to *hash function 86 to produce another 48-bit value*. See *id.* at Fig. 8, 15:21–24; 16:16–19 (“The 48-bit destination address 61 from an incoming packet is simultaneously subjected to *the hash function 86* and a CAM match” (emphasis added)), 16:44–46 (“this compare in the CAM is done in parallel with *the hash function*” (emphasis added)). The application of the hash function and the performance of the hash lookup are two different operations that produce different results. The hash function application produces a hashed 48-bit value, while the hash lookup results in pointing to an entry in the translation table that includes the gigahheader information, for processing the packet. See *id.* at Fig. 8 (identifying hash function 86 applied to input address 85,

resulting in hashed address 89); 15:60–63. Spinney further discloses that the hash *lookup* is performed only if a CAM match is not found and, therefore, must occur *after* the CAM lookup is performed. *Id.* at 16:20–26 (“[I]f a CAM match is found in CAM 23, an index into the translation table 94 is immediately generated as indicated by the line 100. *If not*, the 16-bit field 88 of the hashed address 87 is used to index into the hash table 89” (emphasis added)).

Spinney describes the IR process as performing “the necessary processing to determine if the packet is to be forwarded to the crossbar 12.” *Id.* at 6:17–21. “This decision is made by performing destination address, source address, and protocol field lookups with the aid of the content addressable memory 23 and the internal hash function, according to the invention.” *Id.* at 6:21–25. The invention described is address lookups primarily performed by the hash function, and a CAM lookup for problem addresses and matching of addresses stored in the CAM for filtering. *See id.* at 15:4–8 (“hash lookup is an important feature of the invention”), 16:15–31 (address of incoming packet subjected to hash function 86 and CAM match), 37–47 (CAM comparison for filtering addresses and up to 32 collision addresses). However, Petitioner does not explain, and we do not find any embodiment of Spinney in which the hash lookup and the CAM lookup both proceed in parallel to obtain filtering *and* port forwarding information for the same packet. That is, we find that when there is no match in the CAM Spinney’s hash lookup proceeds to conclusion, and when there is a match in the CAM the hash lookup does not proceed. *Id.* at 9:34–37 (“When a 48-bit destination or 48-bit source address is found as an entry in the CAM 23, the controller inhibits the hash lookup for this value.”); 16:20–25 (describing

that Spinney determines if there is a CAM match, and “[i]f **not**, the 16-bit field 88 of the hashed address 87 is used to index into the hash table 89 to select a hash bucket90, and this selected hash bucket contains a pointer 93 into the translation table 94” (emphasis added)).

Petitioner’s reliance on broad statements in column 6 of Spinney does not persuade us otherwise. During oral argument, Petitioner argued that Spinney broadly describes the IR process as disclosing every limitation, including that the CAM lookup occurs in parallel with the hash lookup. Tr. 50:10–14, 53:12–54:8, 123:5–22. The argument takes Spinney out of context of its disclosure. Column 6 describes the inbound receive process, and, in particular, the decision for packets in the bridge link configuration (bridged packets). Ex. 1004, 6:14–25. Specifically, the passage in column 6 describing the use of the CAM refers to performing address and protocol field lookups. *Id.* This is the process described in detail above, where if the CAM lookup results in a match, the hashed address is not used to obtain the information on how to forward the packet. The passage in column 6 does not disclose that the CAM lookup and the hash lookup are both performed in parallel. To the contrary, we find that this passage describes the operation of the hash lookup as described in Spinney, where the CAM lookup stores a limited number of addresses of interest for filtering, and to avoid hash-bucket collision. The CAM lookup, therefore, is part of the lookup process for determining the forwarding information of the packet. *See, e.g., id.* at 6:26–27 (“The result of the lookup will determine where the packet is to go.”). Indeed, column 6 lists a number of actions on the packet resulting from the lookup, one of them being filtering and discarding the packet. *Id.* at 6:27–32. Spinney, however, does not select the output interface (where

the packet is to go) and, in parallel, determine if the packet is to be filtered. In sum, Spinney performs a hash lookup and a CAM lookup, but these lookups are not performed in parallel, as required by the claims.

The passage in column 16 that Petitioner's counsel alluded to at oral argument is consistent with the disclosures in column 6 and column 9 that Petitioner relies on. Tr. 53:12–54:8. As stated above, the hash *function* applied to the 48-bit address is the operation performed in parallel with the CAM lookup, as described in column 16. Ex. 1004, 16:15–46. If the address is found in the CAM, the lookup is complete. *Id.* If it is not stored in the CAM, the *hashed address* is used to complete the lookup process. *Id.* The CAM is not involved in the hash lookup. *See id.* at 15:19–27 (describing that the 16-bit field of the hashed address is used to index into a table in packet memory 21). Neither the hashed address, nor the filtering or forwarding information associated with an address is stored in the CAM. *See id.* at 5:54–59 (describing that the packet memory stores the translation table, the hash table, and “certain data” corresponding to the addresses matched in the CAM). We find no disclosure in Spinney that supports Petitioner's statement at oral argument that Spinney's CAM stores hashed addresses. *See* Tr. 126:12–17 (arguing that the CAM stores either the 48-bit source and destination addresses or the hashed address). Therefore, none of the passages cited by Petitioner persuade us that Spinney performs the determining and selecting steps in parallel, as required by the language of claim 63.

III. CONCLUSION

We conclude that Petitioner *has not shown* by a preponderance of the evidence that claim 63 of the '853 patent is unpatentable because Spinney does not disclose that “the selecting step is performed in parallel with the determining step.”

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claim 63 of the '853 patent has not been shown to be unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2016-00306
Patent 7,023,853 B1

PETITIONER:

W. Karl Renner
Lauren Degnan
Alex Gelberg
Adam Shartzner
FISH & RICHARDSON P.C.
IPR40963-0004IP4@fr.com
PTABInbound@fr.com
gelberg@fr.com
shartzner@fr.com

PATENT OWNER:

Jon E. Wright
Robert Greene Sterne
Lori A. Gordon
Lestin L. Kenton
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
Jwright-PTAB@skgf.com
Rsterne-PTAB@skgf.com
Lgordon-PTAB@skgf.com
Lkenton-PTAB@skgf.com