Trials@uspto.gov
571-272-7822

Paper 52
Entered: June 1, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ARISTA NETWORKS, INC.,
Petitioner,

v.

CISCO SYSTEMS, INC.,
Patent Owner.

Case IPR2016-00309
Patent 7,224,668 B1

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

CLEMENTS, *Administrative Patent Judge*.

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

I. INTRODUCTION

Arista Networks, Inc. ("Petitioner") filed a Petition requesting *inter partes* review of claims 1–10, 12, 13, 15–28, 30, 31, 33–43, 48, 49, 51–64, 66, 67, and 69–72 ("the challenged claims") of U.S. Patent No. 7,224,668 B1 (Ex. 1001, "the '668 patent"). Paper 1 ("Pet."). Cisco Systems, Inc. ("Patent Owner") filed a Preliminary Response. Paper 7 ("Prelim. Resp.").

On June 11, 2016, we instituted an *inter partes* review of claims 1–10, 12, 13, 15–28, 30, 31, 33–36, 55–64, 66, 67, and 69–72 of the '668 patent. After institution of trial, Patent Owner filed a Patent Owner Response (Paper 18, "PO Resp.") and Petitioner filed a Reply (Paper 33, "Pet. Reply").[1] Petitioner relies on the Declaration of Dr. Bill Lin (Ex. 1002). Patent Owner relies on the Declaration of Dr. Kevin C. Almeroth (Ex. 2006).

Petitioner filed a Motion to Strike (Paper 41) to which Patent Owner filed an Opposition (Paper 48).

Patent Owner filed a Motion to Strike Petitioner's Reply (Paper 42) to which Petitioner filed an Opposition (Paper 44).

An oral hearing was held on March 7, 2017. Paper 49 ("Tr.").

The Board has jurisdiction under 35 U.S.C. § 6. In this Final Written Decision, issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73, we determine that Petitioner has met its burden of showing, by a preponderance of the evidence, that all of the claims for which trial was instituted are unpatentable. Petitioner's Motion to Strike is *dismissed-as-moot*. Patent Owner's Motion to Strike is *dismissed-as-moot*.

---

[1] Patent Owner's Motion to Seal (Paper 20) and Petitioner's Motion to Seal (Paper 35) were granted in our Order of May 7, 2017 (Paper 51).

A. Related Proceedings

The '668 patent is involved in *Cisco Systems, Inc. v. Arista Networks, Inc.*, Case No. 4:14-cv-05343 (N.D. Cal.) and *Cisco Systems, Inc. v. Arista Networks, Inc., Network Devices, Related Software and Components Thereof (II)*, ITC Inv. No. 337-TA-945. Pet. 1; Paper 6, 1. Petitioner also has filed IPR2015-00974 and IPR2015-01710. Paper 6, 1. Petitioner also has filed over a dozen other petitions requesting *inter partes* review of other patents owned by Patent Owner: IPR2015-00973 (U.S. Patent No. 6,377,577), IPR2015-00975 (U.S. Patent No. 8,051,211), IPR2015-00976 (U.S. Patent No. 7,023,853), IPR2015-00978 (U.S. Patent No. 7,340,597), IPR2015-01049 (U.S. Patent No. 6,377,577), IPR2015-01050 (U.S. Patent No. 7,023,853), IPR2016-00018 (U.S. Patent No. 8,051,211), IPR2016-00119 (U.S. Patent No. 7,047,526), IPR2016-00244 (U.S. Patent No. 7,953,886), IPR2016-00303 (U.S. Patent No. 6,377,577), IPR2016-00304 (U.S. Patent No. 7,023,853), IPR2016-00306 (U.S. Patent No. 7,023,853), and IPR2016-00308 (U.S. Patent No. 7,162,537).

B. The '668 patent

The '668 patent relates generally to an internetworking device, such as a router, with improved immunity to denial-of-service ("DoS") attacks. Ex. 1001, Abstract. At the time, a router typically separated its functionality into a data plane, responsible for accepting transit packets at input ports and routing or switching them to output ports, and a control plane, responsible for higher layer functions, such as establishing routing tables. *Id.* at 1:52–59. DoS attacks were commonly directed at the control plane. *Id.* at 1:59–67. Attempts to solve such problems were difficult to administer and could

result in poor performance when control-plane policies were applied not only to control plane packets, but also to transit packets. *Id.* at 2:24–3:2.

To address these and other issues, the '668 patent discloses an internetworking device whose control plane processes are collectively arranged as a single addressable port such that all packets intended for the control plane always pass through this designated port, which thereby provides the ability to better manage control plane traffic. *Id.* at 3:42–50. A set of port services unique to the control plane may be applied to the aggregate control plane port. *Id.* at 3:54–56.

Figure 1 is reproduced below.

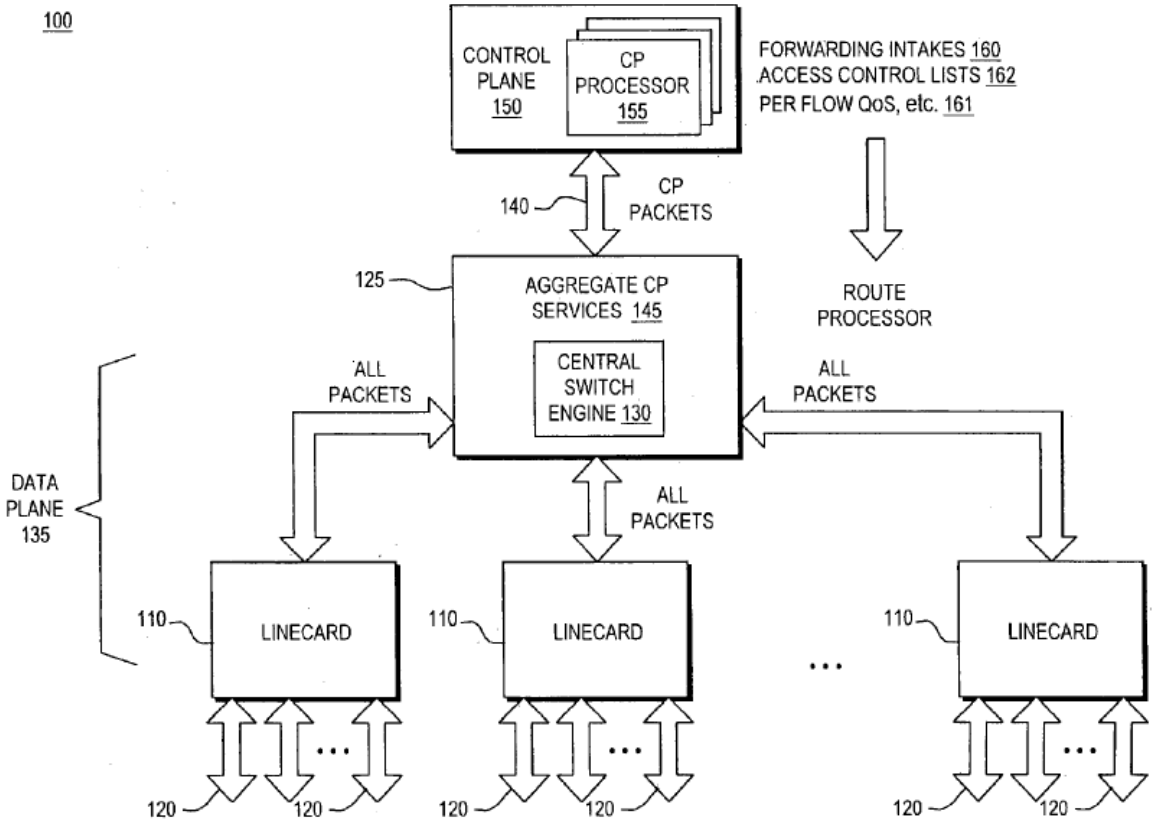

FIG. 1

Figure 1 is a block diagram of internetworking device 100, such as a router, comprising control plane port 140, which defines a single access path

between central switch engine 130 and control plane 150. *Id.* at 4:47–67. Line cards 110 and central switch engine 130 accept packets received on a given port 120 and route them through to another output port 120. *Id.* at 5:5–7. Because all packets destined to control plane 150 pass through central switch engine 130 prior to being routed to functions 155, central switch engine 130 can be used to implement aggregate control plane protection. *Id.* at 5:36–42. Control plane port services determine if a given packet is destined to a control plane process 150. *Id.* at 5:56–58. Control plane port 140 may be a single physical port or may be a virtual address, but either way, it can be treated as a traditional hardware port to which a full range of traditional port control features—e.g., rate limiting, access lists, hierarchical queues based on priority—can be applied to help protect control plane 150 from a DoS attack, or to provide other quality of service ("QoS"). *Id.* at 5:1–4, 5:66–6:44.

C. Illustrative Claim

Of the challenged claims, claims 1, 19, and 55 are independent. Claim 1 is reproduced below:

> 1. An internetworking device comprising:
>
> a. a plurality of physical network interface ports, each for providing a physical connection point to a network for the internetworking device, the ports being configurable by control plane processes;
>
> b. port services, for operating on packets entering and exiting the physical network interface ports, the port services providing an ability to control and monitor packet flows, as defined by control plane configurations;
>
> c. a control plane, comprising a plurality of internetworking control plane processes, the control plane

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.