Trials@uspto.gov
571-272-7822

Paper 8
Date: September 20, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

ORCKIT CORPORATION,
Patent Owner.

IPR2023-00554
Patent 10,652,111 B2

Before KRISTEN L. DROESCH, NATHAN A. ENGELS, and BRENT M. DOUGAL, *Administrative Patent Judges*.

DOUGAL, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background and Summary

Petitioner, Cisco Systems, Inc., requests that we institute an *inter partes* review challenging the patentability of claims 1–9, 12–24, and 27–31 (the "challenged claims") of U.S. Patent 10,652,111 B2 (Ex. 1001, "the '111 patent"). Paper 1 ("Petition" or "Pet."). Patent Owner, Orckit Corp., argues that Petitioner's request is deficient and should not be granted. Paper 6 ("Preliminary Response" or "Prelim. Resp.").

Applying the standard set forth in 35 U.S.C. § 314(a), which requires demonstration of a reasonable likelihood that Petitioner would prevail with respect to at least one challenged claim, we institute an *inter partes* review.[1]

B. Related Matters

The parties identify the following related district court litigation: *Orckit Corp. v. Cisco Systems, Inc.*, No. 2:22-cv-00276 (E.D. Tex.) ("parallel district court proceeding"). Pet. 78; Paper 7, 2.

C. The '111 Patent

The '111 patent is titled "Method and System for Deep Packet Inspection in Software Defined Networks." Ex. 1001, code (54). Deep Packet Inspection ("DPI") is a technique for examining network communications that can be used to extract data patterns from a data communication channel. *Id.* at 1:21–25. The extracted data patterns are useful for a variety of purposes, including network security and data analytics. *Id.*

[1] Our findings and conclusions at this stage are preliminary, and thus, no final determinations are made.

A software defined network ("SDN") is a networking architecture that provides for centralized management of the nodes in a network, as opposed to the distributed architecture utilized by conventional networks. *Id.* at 1:30–38. For example, a SDN may utilize a controller to manage network nodes such as vSwitches. *Id.* SDN-based architectures typically decouple the data forwarding (*e.g.*, data plane) from control decisions (*e.g.*, control plane), such as routing, resources, and other management functionalities. *Id.* at 1:39–49. The decoupling may allow the data plane and the control plane to operate on different hardware, in different runtime environments, and/or operate using different models. *Id.*

Figure 1 shows a method for DPI in an SDN.

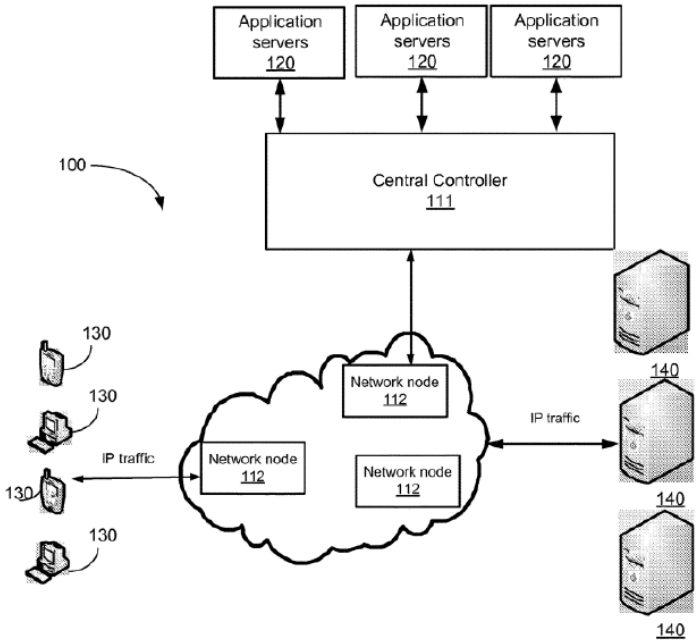

FIG. 1

In the embodiment of Figure 1, above, a network system 100 includes a controller 111 "configured to perform deep packet inspection on designated packets from designated flows or TCP sessions" by "instruct[ing] each of the network nodes 112 which of the packets and/or sessions should be directed to the controller 111 for packet inspections." *Id.* at 4:5–11. The

network node may be instructed to either redirect the packet to controller 111 or send the packet to the destination server 140. *Id*. For example, the controller may send a "probe" instruction to a network node such that, when the network node receives a packet that matches a "packet-applicable criterion," the network node will "mirror" (i.e., send) some or all of the packet to a security component for inspection. *Id.* at 2:3–44.

D. Illustrative Claim(s)

Of the challenged claims, claim 1 is the only independent:

> 1. A method for use with a packet network including a network node for transporting packets between first and second entities under control of a controller that is external to the network node, the method comprising:
>
> sending, by the controller to the network node over the packet network, an instruction and a packet-applicable criterion;
>
> receiving, by the network node from the controller, the instruction and the criterion;
>
> receiving, by the network node from the first entity over the packet network, a packet addressed to the second entity;
>
> checking, by the network node, if the packet satisfies the criterion;
>
> responsive to the packet not satisfying the criterion, sending, by the network node over the packet network, the packet to the second entity; and
>
> responsive to the packet satisfying the criterion, sending the packet, by the network node over the packet network, to an entity that is included in the instruction and is other than the second entity.

Ex. 1001, 10:52–11:4.

E. Evidence

Petitioner's grounds of unpatentability rely on the following evidence:

Name	Patent Document	Exhibit
Lin	US 9,264,400 Bl (Feb. 16, 2016)	1005
Swenson	US 2013/0322242 Al (Dec. 5, 2013)	1007
Shieh	US 2013/0291088 Al (Oct. 31, 2013)	1006

F. Prior Art and Asserted Grounds

Petitioner asserts the following grounds of unpatentability (Pet. 4–5), supported by the declaration of Samrat Bhattacharjee, Ph.D. (Ex. 1004):

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–9, 12–24, 27–31	103	Lin, Swenson
1, 5–9, 12–24, 27–30	103	Shieh, Swenson

II. DISCRETION UNDER 35 U.S.C. § 314(A)

Patent Owner contends the Board should exercise its discretion to deny institution under 35 U.S.C. § 314, citing the discretionary-denial factors articulated in *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential) ("*Fintiv*"). *See* Prelim. Resp. 23–36. More specifically, Patent Owner contends that consideration of the *Fintiv* factors weigh in favor of discretionary denial. *Id.* Petitioner disagrees. Pet. 74–77.

Under § 314(a), the Director has discretion to deny institution of an *inter partes* review, and that discretion has been delegated to the Board. *See* 37 C.F.R. § 42.4(a) ("The Board institutes the trial on behalf of the Director."); *SAS Inst. v. Iancu*, 138 S. Ct. 1348, 1356 (2018) ("[Section] 314(a) invests the Director with discretion on the question whether to institute review . . . ." (emphasis omitted)).

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.