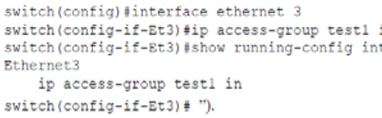
US 7,224,668	Cisco	Arista
Claim 1		
[1.0] An internetworking device comprising: a. a plurality of physical network interface ports, each for providing a physical connection point to a network for the internetworking device, the ports being configurable by control plane processes;	Cisco devices, at least the Cisco 7500 Series, include an internetworking device comprising 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. See, e.g., Control Plane Policing Implementation Best Practices available at http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html (Ex. 2016) ("IP networks provide users with connectivity to networked resources such as corporate servers, extranet partners, multimedia content, the Internet, and any other application envisioned within IP networks. While these networks function to carry data plane (user-generated) packets, they are also created and operated by control plane and management plane packets."). Cisco devices, at least the Nexus 7000 Series, include an internetworking device comprising 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. See, e.g., Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x (Modified 4/16/14) (Ex. 2017) at p. 646 ("Control plane—Handles all routing protocol control	Arista switches, including at l 7050, 7050X, 7150, 7250X, 7 and 7500E series models, and including at least version 4.14 internetworking device compr physical network interface po providing a physical connecti network for the internetworki being configurable by control See, e.g., Arista Configuration Rev. 2 (10/2/14) (Ex. 2024) a Networks features switches w non-blocking 100/1000Mb an Ethernet ports that are control extensible modular network o See, e.g., Arista Configuration Rev. 2 (10/2/14) (Ex. 2024) a control plane builds and main table"). See, e.g., Arista Conf 4.14.3F - Rev. 2 (10/2/14) (Ex ("The data plane routes IP pac information derived by the co e.g., Arista Configuration Gui 2 (10/2/14) (Ex. 2024) at p. 6 plane command places the sw plane configuration mode."). 7508E Image available at http://www.arista.com/assets/ 8- specifications.png (Ex. 202

US 7,224,668	Cisco	Arista
	traffic.”). Cisco devices, at least the Catalyst 6500, include an internetworking device comprising 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. See, e.g., Cisco IOS Software Configuration Guide, Release 12.2(33)SXH and Later Releases (2007-2012) (Ex. 2018) at p. 53-2 (“The majority of traffic managed by the RP is handled by way of the control and management planes.”). See, e.g., Control Plane Policing Implementation Best Practices available at http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html (Ex. 2016) (“IP networks provide users with connectivity to networked resources such as corporate servers, extranet partners, multimedia content, the Internet, and any other application envisioned within IP networks. While these networks function to carry data plane (user-generated) packets, they are also created and operated by control plane and management plane packets.”).	
[1.1] b. port services, for operating on packets entering and exiting the physical network interface	Cisco devices, at least the Cisco 7500 Series, include 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	Arista switches, including at l 7050, 7050X, 7150, 7250X, 7 and 7500E series models, and including at least version 4.14 services, for operating on pac

US 7,224,668	Cisco	Arista
ports, the port services providing an ability to control and monitor packet flows, as defined by control plane configurations;	defined by control plane configurations. See, e.g., Control Plane Policing Implementation Best Practices available at http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html (Ex. 2016) ("Interface ACL – The interface access control list (iACL) is the traditional and most generally available approach for managing all packets entering or exiting a network device. The iACLs are well understood and are generally applicable to data, services, control, and management plane packets. However, as illustrated in Figure 2, iACLs are applied at the interface level to each packet ingressing (or egressing) the interface—not just control plane packets, for example."). Cisco devices, at least the Nexus 7000 Series, include 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. See, e.g., Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x (Modified 4/16/14) (Ex. 2017) at p. 455 ("You can apply an IPv4 or IPv6 ACL to a Layer 2 interface, which can be a physical port or a port channel. ACLs applied to these interface types are considered port ACLs.").	exiting the physical network i port services providing an abi monitor packet flows, as defin configurations. See, e.g., Arista Configuration Rev. 2 (10/2/14) (Ex. 2024) a plane routes IP packets based derived by the control plane." Configuration Guide v. 4.14.3 (Ex. 2024) at p. 835 ("ACL, P Prefix List Introduction An ac (ACL) is an ordered set of rul inbound flow of packets into I port channel interfaces or the plane. The switch supports th a wide variety of filtering crit and MAC addresses, TCP/UD include/exclude options witho its performance or feature set. Configuration Guide v. 4.14.3 (Ex. 2024) at p. 848. These commands assign test1 interface, then verifies the ass  switch(config)#interface ethernet 3 switch(config-if-Et3)#ip access-group test1 i switch(config-if-Et3)#show running-config int Ethernet3 ip access-group test1 in switch(config-if-Et3)# "). See, e.g., Arista Configuration Rev. 2 (10/2/14) (Ex. 2024) a

US 7,224,668	**Cisco**	**Arista**
	See, e.g., Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide (April 2014) (Ex. 2020) at p. 2-17 (“A QoS policy attached to the physical port takes effect when the port is not a member of a port channel.”). Cisco devices, at least the Catalyst 6500, include 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. See, e.g., Cisco IOS Software Configuration Guide, Release 12.2(33)SXH and Later Releases (2007-2012) (Ex. 2018) at p. 51-2 (“Port ACLs perform access control on all traffic entering the specified Layer 2 port.”). See, e.g., Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2, Quality of Service Overview (Ex. 2021) at p. QC-6 (“Policies can be set that include classification based on physical port….”). See, e.g., Control Plane Policing Implementation Best Practices available at http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html (Ex. 2016) (“Interface ACL – The interface access control list (iACL) is the traditional and most generally available approach for managing all packets entering or exiting a network device. The iACLs are well	of Service Conceptual Overvi apply to traffic that flows thro and control planes. These pro data fields (CoS or DSCP) or to traffic classes for prioritize Transmission queues are conf individual Ethernet ports to sh its traffic class. Many switche traffic policies that apply to d access control lists.”).

US 7,224,668	Cisco	Arista
	understood and are generally applicable to data, services, control, and management plane packets. However, as illustrated in Figure 2, iACLs are applied at the interface level to each packet ingressing (or egressing) the interface—not just control plane packets, for example.).	
[1.2] c. a control plane, comprising a plurality of internetworking control plane processes, the control plane processes for providing high-level control and configuration of the ports and the port services;	Cisco devices, at least the Cisco 7500 Series, include a control plane, comprising a plurality of internetworking control plane processes, the control plane processes for providing high-level control and configuration of the ports and the port services. See, e.g., Control Plane Policing Implementation Best Practices available at http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html (Ex. 2016) ("IP networks provide users with connectivity to networked resources such as corporate servers, extranet partners, multimedia content, the Internet, and any other application envisioned within IP networks. While these networks function to carry data plane (user-generated) packets, they are also created and operated by control plane and management plane packets."). Cisco devices, at least the Nexus 7000 Series, include a control plane, comprising a plurality of internetworking control plane processes, the control plane processes for providing high-level control and configuration of the ports and the port	Arista switches, including at l 7050, 7050X, 7150, 7250X, 7 and 7500E series models, and including at least version 4.14 control plane, comprising a pl internetworking control plane control plane processes for pr control and configuration of t services. See, e.g., Arista Configuratio Rev. 2 (10/2/14) (Ex. 2024) a control plane builds and main table"). See, e.g., Arista Whit Switch Architecture (March 2 p. 2 ("Supervisor modules on switches are used for control- management-plane functions

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.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**