IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

	§	
WINTERSPRING DIGITAL LLC,	§	
	§	Case No.
Plaintiff,	§	
	§	**JURY TRIAL DEMANDED**
v.	§	
	§	
EXTREME NETWORKS, INC.,	§	
	§	
Defendant.	§	
	§	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Winterspring Digital LLC ("Winterspring" or "Plaintiff") for its Complaint against Extreme Networks, Inc. ("Extreme" or "Defendant") alleges as follows:

THE PARTIES

1. Winterspring is a limited liability company organized and existing under the laws of the State of Texas, with its principal place of business located at 104 East Houston Street, Marshall, Texas 75670.

2. Upon information and belief, Defendant Extreme is a Delaware corporation that maintains regular and established places of business throughout Texas, for example, at its facilities in this District at 6 Wiltshire Ct., Lucas, TX 75002. Extreme is registered to conduct business in the State of Texas and has appointed CT Corporation System, located at 1999 Bryan ST., Ste. 900, Dallas, TX 75201 as its agent for service of process. Extreme is a leading manufacturer and seller of computer equipment in the world and in the United States. Upon information and belief, Extreme does business in Texas and in the Eastern District of Texas, directly or through intermediaries.

JURISDICTION

3. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq*. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

4. This Court has personal jurisdiction over Defendant. Defendant regularly conducts business and has committed acts of patent infringement and/or has induced acts of patent infringement by others in this Judicial District and/or has contributed to patent infringement by others in this Judicial District, the State of Texas, and elsewhere in the United States.

5. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1400(b) and 1391(b) and (c) because, among other things, Defendant is subject to personal jurisdiction in this Judicial District, has a regular and established place of business in this Judicial District, has purposely transacted business involving the accused products in this Judicial District, including sale to one or more customers in Texas, and certain of the acts complained herein, including acts of patent infringement, occurred in this Judicial District.

6. Defendant is subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to its substantial business in this State and Judicial District, including (a) at least part of its past infringing activities, (b) regularly doing or soliciting business in Texas, and/or (c) engaging in persistent conduct and/or deriving substantial revenue from goods and services provided to customers in Texas.

PATENTS-IN-SUIT

7. On January 16, 2007, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,164,692 (the "'692 Patent") entitled "Apparatus and Method for

Transmitting 10 Gigabit Ethernet LAN Signals Over a Transport System." A true and correct copy of the '692 Patent is available at http://pdfpiw.uspto.gov/.piw?docid=7164692.

8. On October 4, 2011, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,032,646 (the "'646 Patent") entitled "Administering a Communication Network." A true and correct copy of the '646 Patent is available at http://pdfpiw.uspto.gov/.piw?docid=8032646.

9. On September 2, 2008, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,420,975 (the "'975 Patent") entitled "Method and Apparatus For High-Speed Frame Tagger." A true and correct copy of the '975 Patent is available at http://pdfpiw.uspto.gov/.piw?docid=7420975.

10. Winterspring is the sole and exclusive owner of all right, title, and interest in the '692, '646, and '975 Patents (the "Patents-in-Suit") and holds the exclusive right to take all actions necessary to enforce its rights to the Patent-in-Suit, including the filing of this patent infringement lawsuit. Winterspring also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

FACTUAL ALLEGATIONS

11. The Patents-in-Suit generally cover systems and methods for routing data over a network.

12. The '692 Patent generally discloses an apparatus and method for transmitting LAN signals over a transport system. A system sends or receives a signal to or from a transport system, converts the signal to an intermediate form, re-clocks the intermediate signal, reconverts and then transmits the signal. The technology described in the '692 Patent was developed by Jeffrey Lloyd Cox and Samir Satish Seth. By way of example, this technology is implemented today in servers,

computers, network switches, modules, and transceivers that receive, convert, monitor, and send 10-Gigabit LAN signals.

13. The ’646 Patent discloses systems and methods for routing traffic through a network with the use of a GUI. The technology described in the ’646 Patent was developed by Siddhartha Nag, Alfred D’Souza, Naveed Alam, and Rakesh Patel of Prom KS Limited Liability Company. By way of example, this technology is implemented today in hardware and software which allow a user with a GUI to optimize routing decisions.

14. The ’975 Patent discloses an apparatus and methods for examining a packet, determining a protocol type and tagging the packet. The technology described in the ’975 Patent was developed by Velamur Krishnamachari and Dinesh Annayya from Cypress Semiconductor Corporation. By way of example, this technology is implemented today in servers, computers, network switches, modules and software which implement packet tagging.

15. Extreme has infringed and is continuing to infringe the Patents-in-Suit by making, using, offering to sell, selling, and/or importing products which implement the technology disclosed in the above Patents-in-Suit.

COUNT I
(Infringement of the ’692 Patent)

16. Paragraphs 1 through 15 are incorporated by reference as if fully set forth herein.

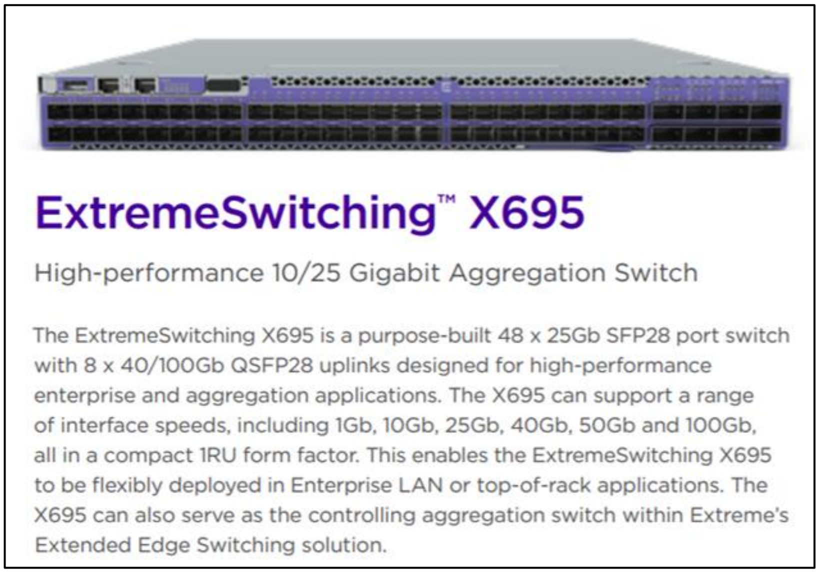
17. Winterspring has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the ’692 Patent.

18. Defendant has and continues to directly infringe the ’692 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’692 Patent. Such products include, but are not

limited to servers, computers, network switches, modules, and transceivers that receive, convert, monitor, and send 10-Gigabit LAN signals.

19. For example, Defendant has and continues to directly infringe at least claim 10 of the ’692 Patent by making, using, offering to sell, selling, and/or importing into the United States products that receive, convert, and monitor 10GE LAN signals.

20. For example, the Extreme X695 performs a method of transferring 10GE LAN client signals from a transport system to a client system comprising receiving the 10GE LAN client signal transmitted over the transport system, converting the 10GE LAN client signal to an intermediate signal, recovering clock data from the intermediate signal, recovering a data stream from the intermediate signal, reconverting the intermediate signal to the 10GE LAN client signal; transferring the 10GE LAN client signal to a client system; and monitoring the intermediate form with a monitoring device wherein the monitoring device is a 10GE LAN media access controller.



ExtremeSwitching™ X695

High-performance 10/25 Gigabit Aggregation Switch

The ExtremeSwitching X695 is a purpose-built 48 x 25Gb SFP28 port switch with 8 x 40/100Gb QSFP28 uplinks designed for high-performance enterprise and aggregation applications. The X695 can support a range of interface speeds, including 1Gb, 10Gb, 25Gb, 40Gb, 50Gb and 100Gb, all in a compact 1RU form factor. This enables the ExtremeSwitching X695 to be flexibly deployed in Enterprise LAN or top-of-rack applications. The X695 can also serve as the controlling aggregation switch within Extreme's Extended Edge Switching solution.[1]

21. Defendant has and continues to indirectly infringe one or more claims of the ’692 Patent by knowingly and intentionally inducing others, including Extreme customers and end-

[1] https://www.extremenetworks.com/products/switches/extremexos-switches/x695.

users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that receive, convert, monitor, and send 10GE LAN signals.

22. Defendant, with knowledge that these products, or the use thereof, infringe the ’692 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’692 Patent by providing these products to end users for use in an infringing manner. Alternatively, on information and belief, Defendant has adopted a policy of not reviewing the patents of others, including specifically those related to Defendant’s specific industry, thereby remaining willfully blind to the Patent-in-Suit at least as early as the issuance of the Patents-in-Suit.

23. Defendant induced infringement by others, including customers and end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end users, infringe the ’692 Patent, but while remaining willfully blind to the infringement. Defendant has and continues to induce infringement by its customers and end-users by supplying them with instructions on how to operate the Accused Instrumentalities in an infringing manner, while also making publicly available information on the Accused Instrumentalities via Defendant’s website and other publications. Upon information and belief, Defendant provides product support to its customers and end-users, where Defendant further instructs them to use the Accused Instrumentalities in an infringing manner.

24. Winterspring has suffered damages as a result of Defendant’s direct and indirect infringement of the ’692 Patent in an amount to be proved at trial.

25. Winterspring has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '692 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

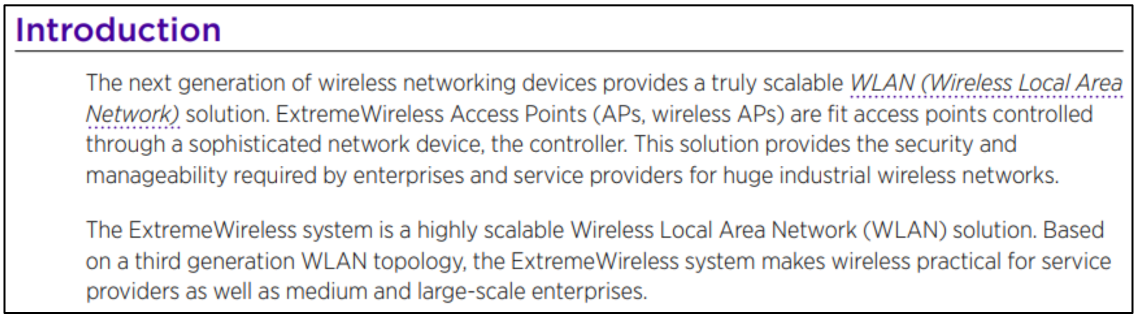
COUNT II
(Infringement of the '646 Patent)

26. Paragraphs 1 through 15 are incorporated by reference as if fully set forth herein.

27. Winterspring has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the '646 Patent.

28. Defendant has and continues to directly infringe the '646 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '646 Patent. Such products include, but are not limited to, computers, network switches, modules, and software that perform packet tagging.

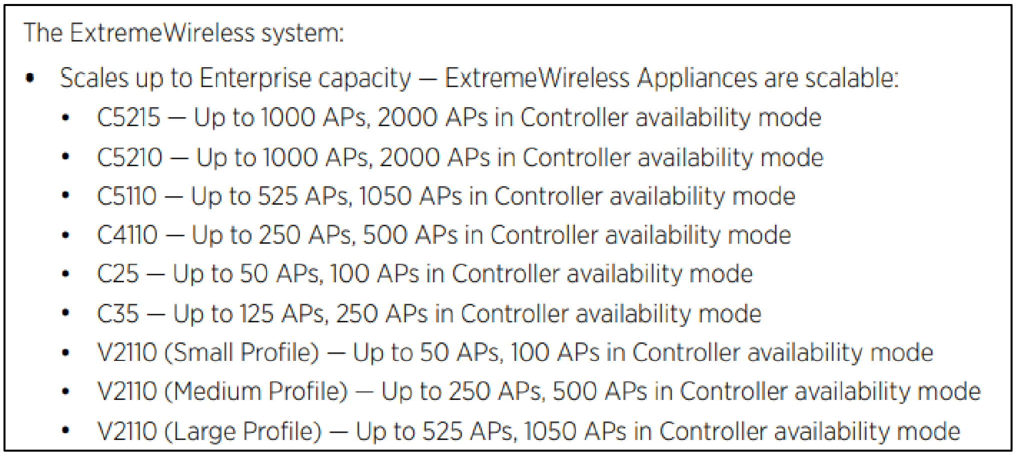
29. For example, Defendant has and continues to directly infringe at least claim 5 of the '975 Patent by making, using, offering to sell, selling, and/or importing into the United States products that perform packet tagging, including, but not limited to, the ExtremeWireless V10.41.01.



Introduction

The next generation of wireless networking devices provides a truly scalable *WLAN (Wireless Local Area Network)* solution. ExtremeWireless Access Points (APs, wireless APs) are fit access points controlled through a sophisticated network device, the controller. This solution provides the security and manageability required by enterprises and service providers for huge industrial wireless networks.

The ExtremeWireless system is a highly scalable Wireless Local Area Network (WLAN) solution. Based on a third generation WLAN topology, the ExtremeWireless system makes wireless practical for service providers as well as medium and large-scale enterprises.

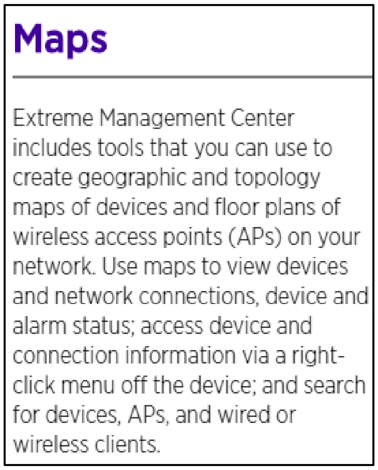


The ExtremeWireless system:

- Scales up to Enterprise capacity — ExtremeWireless Appliances are scalable:
  - C5215 — Up to 1000 APs, 2000 APs in Controller availability mode
  - C5210 — Up to 1000 APs, 2000 APs in Controller availability mode
  - C5110 — Up to 525 APs, 1050 APs in Controller availability mode
  - C4110 — Up to 250 APs, 500 APs in Controller availability mode
  - C25 — Up to 50 APs, 100 APs in Controller availability mode
  - C35 — Up to 125 APs, 250 APs in Controller availability mode
  - V2110 (Small Profile) — Up to 50 APs, 100 APs in Controller availability mode
  - V2110 (Medium Profile) — Up to 250 APs, 500 APs in Controller availability mode
  - V2110 (Large Profile) — Up to 525 APs, 1050 APs in Controller availability mode

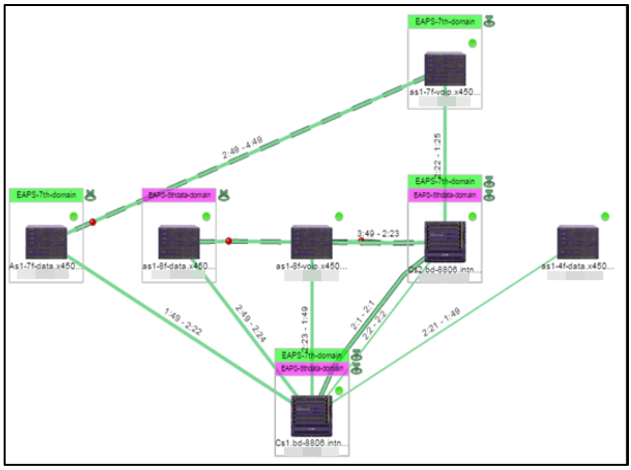
- Integrates with the Extreme Networks Extreme Management Center Suite of products. For more information, see Extreme Networks Extreme Management Center Integration on page 18.

[2]



Maps

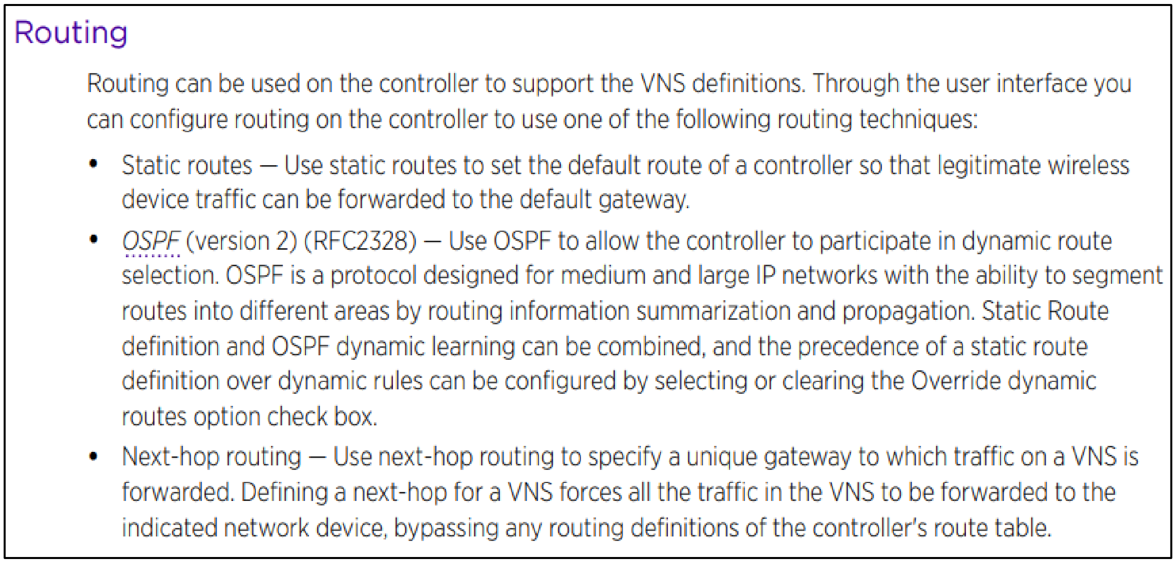
Extreme Management Center includes tools that you can use to create geographic and topology maps of devices and floor plans of wireless access points (APs) on your network. Use maps to view devices and network connections, device and alarm status; access device and connection information via a right-click menu off the device; and search for devices, APs, and wired or wireless clients.



[3]

[2] https://content.etilize.com/User-Manual/1044537499.pdf, page 17 of 708.

[3] https://emc.extremenetworks.com/content/oneview/docs/network/devices/docs/maps/l_ov_map_tab.htm#LinkInformation.



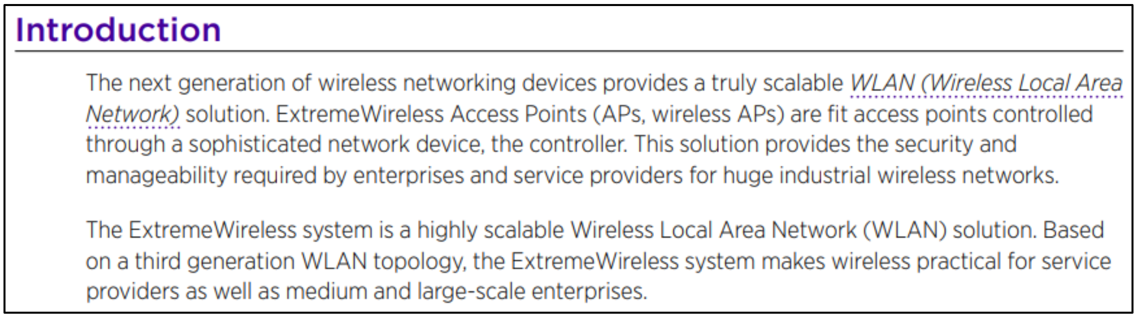
Routing

Routing can be used on the controller to support the VNS definitions. Through the user interface you can configure routing on the controller to use one of the following routing techniques:

- Static routes — Use static routes to set the default route of a controller so that legitimate wireless device traffic can be forwarded to the default gateway.
- OSPF (version 2) (RFC2328) — Use OSPF to allow the controller to participate in dynamic route selection. OSPF is a protocol designed for medium and large IP networks with the ability to segment routes into different areas by routing information summarization and propagation. Static Route definition and OSPF dynamic learning can be combined, and the precedence of a static route definition over dynamic rules can be configured by selecting or clearing the Override dynamic routes option check box.
- Next-hop routing — Use next-hop routing to specify a unique gateway to which traffic on a VNS is forwarded. Defining a next-hop for a VNS forces all the traffic in the VNS to be forwarded to the indicated network device, bypassing any routing definitions of the controller's route table.

[4]

30. For example, the ExtremeWireless V10.41.01 performs a method comprising the step of displaying, via a graphical user interface (GUI) on a display, a graphical representation of a plurality of nodes available in a network, wherein the plurality of nodes comprises a first edge node and a second edge node, wherein the plurality of nodes further comprises a plurality of router nodes located between the first edge node and the second edge node.

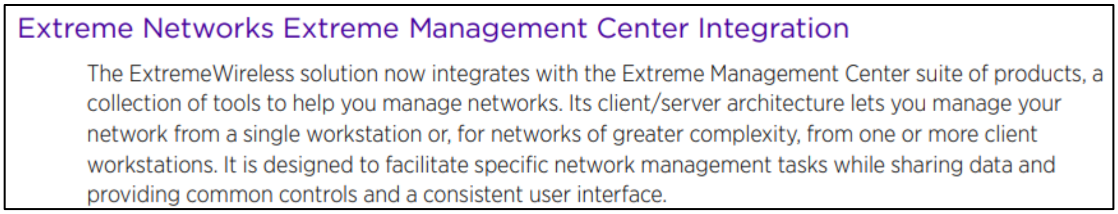


Introduction

The next generation of wireless networking devices provides a truly scalable *WLAN (Wireless Local Area Network)* solution. ExtremeWireless Access Points (APs, wireless APs) are fit access points controlled through a sophisticated network device, the controller. This solution provides the security and manageability required by enterprises and service providers for huge industrial wireless networks.

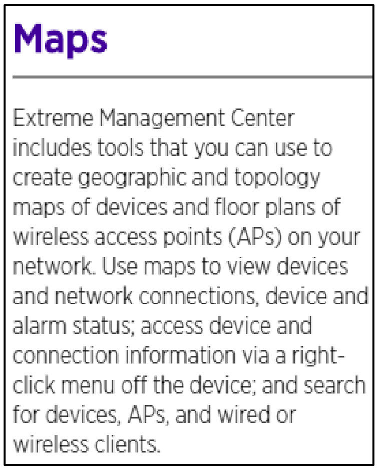
The ExtremeWireless system is a highly scalable Wireless Local Area Network (WLAN) solution. Based on a third generation WLAN topology, the ExtremeWireless system makes wireless practical for service providers as well as medium and large-scale enterprises.

[4] https://content.etilize.com/User-Manual/1044537499.pdf, page 28 of 708.



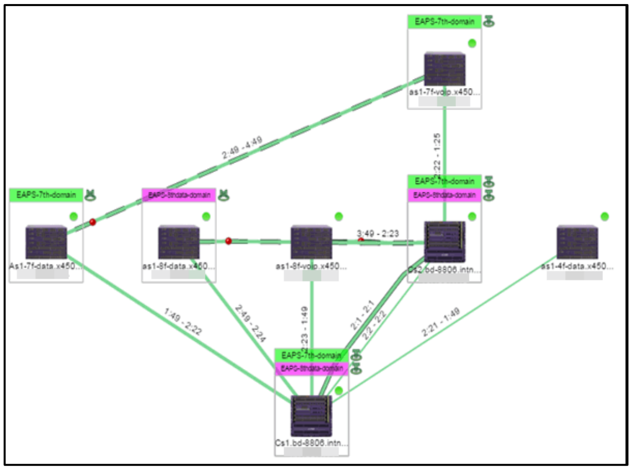
Extreme Networks Extreme Management Center Integration

The ExtremeWireless solution now integrates with the Extreme Management Center suite of products, a collection of tools to help you manage networks. Its client/server architecture lets you manage your network from a single workstation or, for networks of greater complexity, from one or more client workstations. It is designed to facilitate specific network management tasks while sharing data and providing common controls and a consistent user interface.[5]



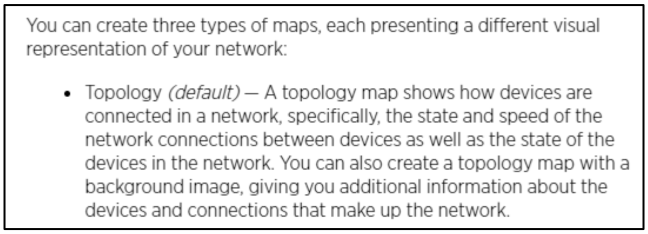
Maps

Extreme Management Center includes tools that you can use to create geographic and topology maps of devices and floor plans of wireless access points (APs) on your network. Use maps to view devices and network connections, device and alarm status; access device and connection information via a right-click menu off the device; and search for devices, APs, and wired or wireless clients.



[6]

31. The topology map shows the network devices in the network topology. It includes two edge devices (first and second) and the path between two includes plurality of router nodes in between.

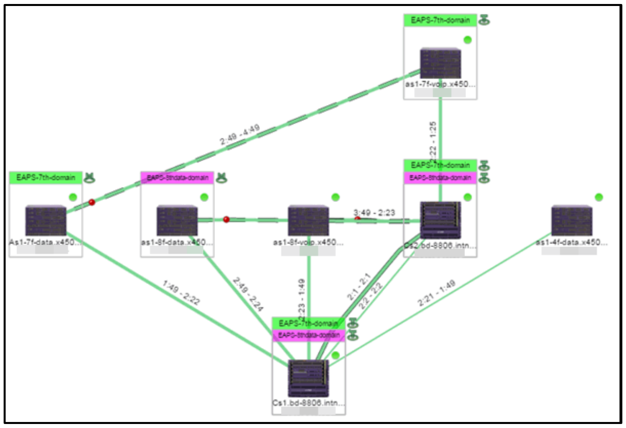


You can create three types of maps, each presenting a different visual representation of your network:

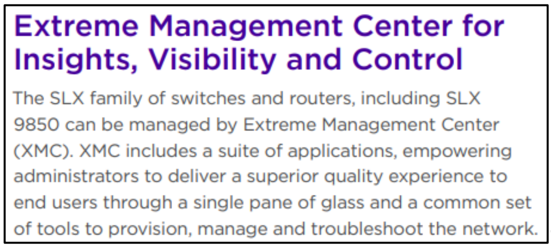
- Topology *(default)* — A topology map shows how devices are connected in a network, specifically, the state and speed of the network connections between devices as well as the state of the devices in the network. You can also create a topology map with a background image, giving you additional information about the devices and connections that make up the network.

[5] Extreme Wireless V10.41.01 User Guide https://content.etilize.com/User-Manual/1044537499.pdf , page 17, 18 of 708.

[6] https://emc.extremenetworks.com/content/oneview/docs/network/devices/docs/maps/l_ov_map_tab.htm#LinkInformation.

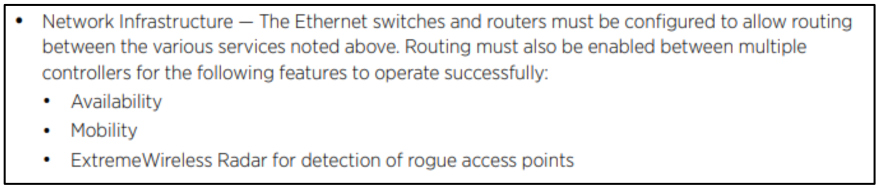


[7]



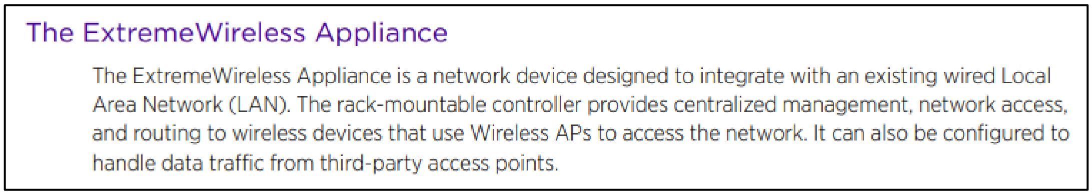
Extreme Management Center for Insights, Visibility and Control

The SLX family of switches and routers, including SLX 9850 can be managed by Extreme Management Center (XMC). XMC includes a suite of applications, empowering administrators to deliver a superior quality experience to end users through a single pane of glass and a common set of tools to provision, manage and troubleshoot the network. [8]



- Network Infrastructure — The Ethernet switches and routers must be configured to allow routing between the various services noted above. Routing must also be enabled between multiple controllers for the following features to operate successfully:
  - Availability
  - Mobility
  - ExtremeWireless Radar for detection of rogue access points

[9]



The ExtremeWireless Appliance

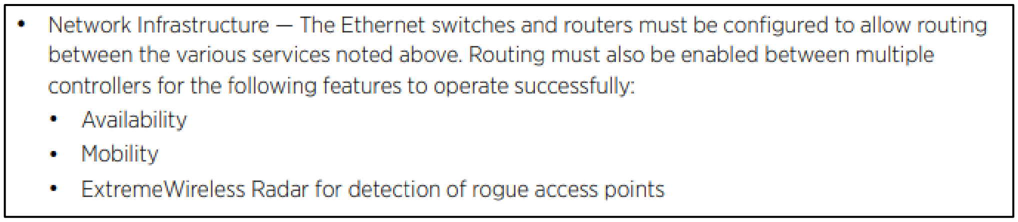
The ExtremeWireless Appliance is a network device designed to integrate with an existing wired Local Area Network (LAN). The rack-mountable controller provides centralized management, network access, and routing to wireless devices that use Wireless APs to access the network. It can also be configured to handle data traffic from third-party access points. [10]

[7] https://emc.extremenetworks.com/content/oneview/docs/network/devices/docs/maps/l_ov_map_tab.htm#link.

[8] https://cloud.kapostcontent.net/pub/7f7d49da-12c2-489f-a437-07a680ab7d47/slx-9850-router-data-sheet.pdf?kui=YT6wq30GcyrRVSzufvHu0w.

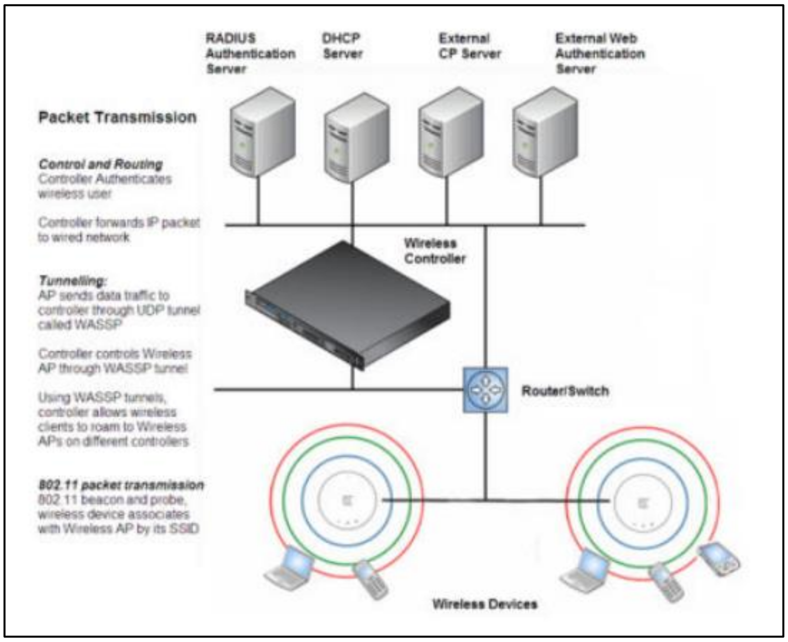
[9] https://content.etilize.com/User-Manual/1044537499.pdf , page 20 of 708.

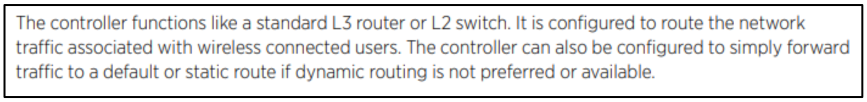
[10] https://content.etilize.com/User-Manual/1044537499.pdf, page 14 of 708.



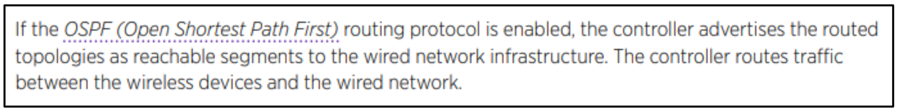
- Network Infrastructure — The Ethernet switches and routers must be configured to allow routing between the various services noted above. Routing must also be enabled between multiple controllers for the following features to operate successfully:
  - Availability
  - Mobility
  - ExtremeWireless Radar for detection of rogue access points

[11]


RADIUS Authentication Server
DHCP Server
External CP Server
External Web Authentication Server
Packet Transmission
Control and Routing
Controller Authenticates wireless user
Controller forwards IP packet to wired network
Wireless Controller
Tunnelling:
AP sends data traffic to controller through UDP tunnel called WASSP
Controller controls Wireless AP through WASSP tunnel
Router/Switch
Using WASSP tunnels, controller allows wireless clients to roam to Wireless APs on different controllers
802.11 packet transmission
802.11 beacon and probe, wireless device associates with Wireless AP by its SSID
Wireless Devices



The controller functions like a standard L3 router or L2 switch. It is configured to route the network traffic associated with wireless connected users. The controller can also be configured to simply forward traffic to a default or static route if dynamic routing is not preferred or available.

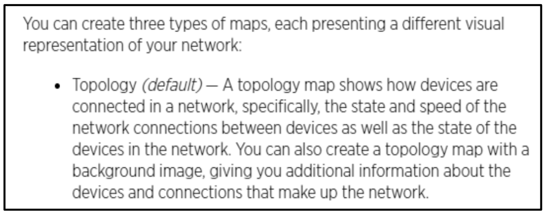


If the *OSPF (Open Shortest Path First)* routing protocol is enabled, the controller advertises the routed topologies as reachable segments to the wired network infrastructure. The controller routes traffic between the wireless devices and the wired network.

32. For example, the displaying, via the GUI, a graphical representation of a plurality of paths available on the network between the first edge node and the second edge node on the network, wherein each of the plurality of paths passes through at least a subset of the plurality of router nodes, wherein the plurality of paths are displayed in a prioritized fashion in accordance with a difference in a number of nodes in each path of the plurality of paths through which traffic between the first edge node and the second edge node will pass if selected. When the edge nodes

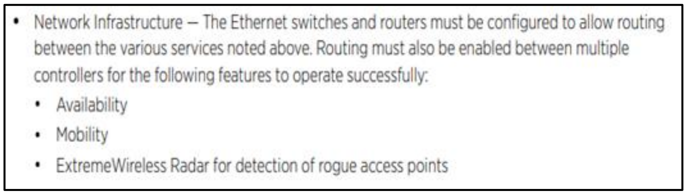
[11] https://content.etilize.com/User-Manual/1044537499.pdf , page 20, 21,23 of 708.

are defined, multiple paths are shown from the source edge node to the destination edge node.

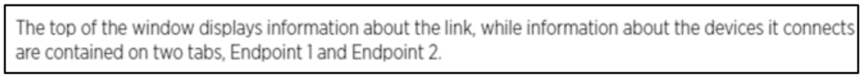


You can create three types of maps, each presenting a different visual representation of your network:

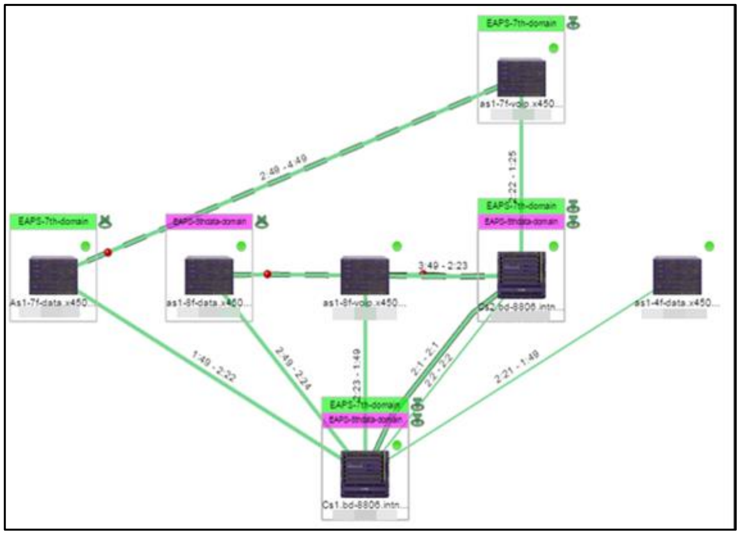
- Topology *(default)* — A topology map shows how devices are connected in a network, specifically, the state and speed of the network connections between devices as well as the state of the devices in the network. You can also create a topology map with a background image, giving you additional information about the devices and connections that make up the network.



- Network Infrastructure — The Ethernet switches and routers must be configured to allow routing between the various services noted above. Routing must also be enabled between multiple controllers for the following features to operate successfully:
  - Availability
  - Mobility
  - ExtremeWireless Radar for detection of rogue access points



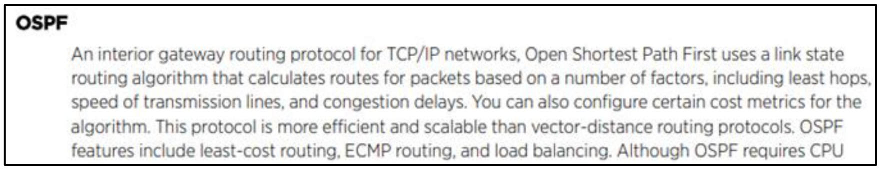
The top of the window displays information about the link, while information about the devices it connects are contained on two tabs, Endpoint 1 and Endpoint 2.[12]



[13]

[12] https://content.etilize.com/User-Manual/1044537499.pdf, page 20, 21,23 of 708.

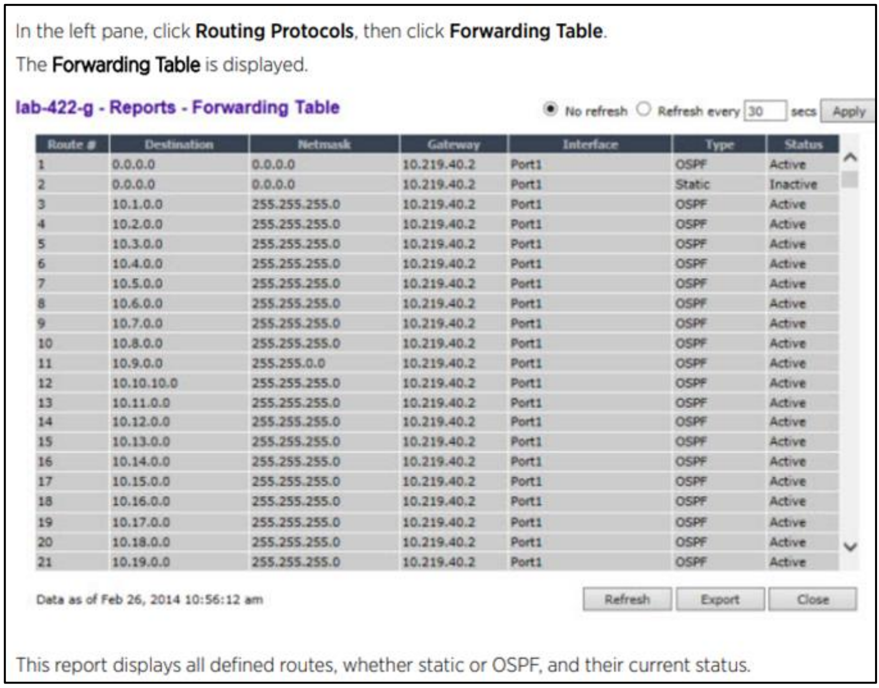
[13] https://emc.extremenetworks.com/content/oneview/docs/network/devices/docs/maps/l_ov_map_tab.htm#link.



OSPF

An interior gateway routing protocol for TCP/IP networks, Open Shortest Path First uses a link state routing algorithm that calculates routes for packets based on a number of factors, including least hops, speed of transmission lines, and congestion delays. You can also configure certain cost metrics for the algorithm. This protocol is more efficient and scalable than vector-distance routing protocols. OSPF features include least-cost routing, ECMP routing, and load balancing. Although OSPF requires CPU [14]

33. When the edge nodes are defined, multiple paths are shown from the source edge node to the destination edge node.



In the left pane, click **Routing Protocols**, then click **Forwarding Table**.

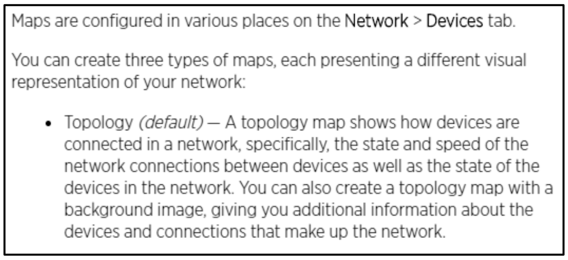
The **Forwarding Table** is displayed.

lab-422-g - Reports - Forwarding Table

Route #	Destination	Netmask	Gateway	Interface	Type	Status
1	0.0.0.0	0.0.0.0	10.219.40.2	Port1	OSPF	Active
2	0.0.0.0	0.0.0.0	10.219.40.2	Port1	Static	Inactive
3	10.1.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
4	10.2.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
5	10.3.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
6	10.4.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
7	10.5.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
8	10.6.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
9	10.7.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
10	10.8.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
11	10.9.0.0	255.255.0.0	10.219.40.2	Port1	OSPF	Active
12	10.10.10.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
13	10.11.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
14	10.12.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
15	10.13.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
16	10.14.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
17	10.15.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
18	10.16.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
19	10.17.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
20	10.18.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
21	10.19.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active

Data as of Feb 26, 2014 10:56:12 am

This report displays all defined routes, whether static or OSPF, and their current status. [15]

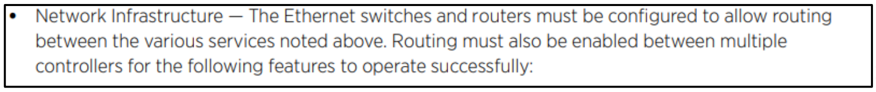


Maps are configured in various places on the **Network** > **Devices** tab.

You can create three types of maps, each presenting a different visual representation of your network:

- Topology *(default)* — A topology map shows how devices are connected in a network, specifically, the state and speed of the network connections between devices as well as the state of the devices in the network. You can also create a topology map with a background image, giving you additional information about the devices and connections that make up the network.

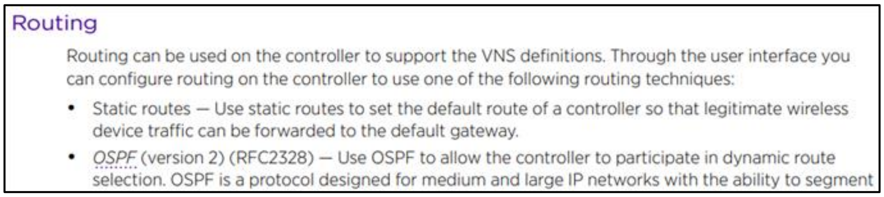
[14] https://content.etilize.com/User-Manual/1044537499.pdf , page 60, 707 of 708.
[15] https://content.etilize.com/User-Manual/1044537499.pdf , page 60, 61 of 708.



- Network Infrastructure — The Ethernet switches and routers must be configured to allow routing between the various services noted above. Routing must also be enabled between multiple controllers for the following features to operate successfully:

[16]

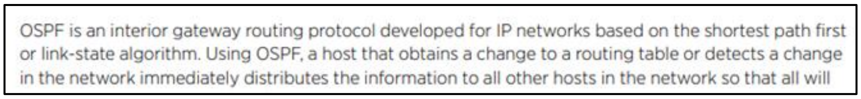
34. When the OSPF routing is selected it is the priority method followed for routing and is based on shortest route with minimum cost. Also, OSPF calculates paths based on least hop factor (least nodes). As shown, the user can access the forwarding table which shows routes (OSPF and static route, OSPF being active path) for same destination. However, priority will be given to path with least hops if OSPF is selected by user (first input).



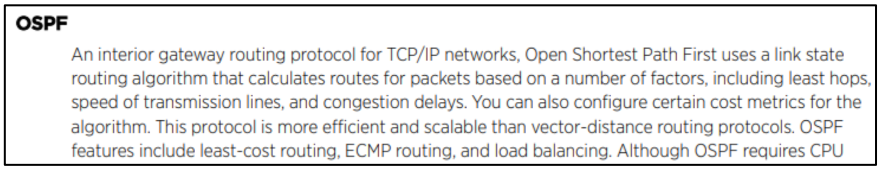
Routing

Routing can be used on the controller to support the VNS definitions. Through the user interface you can configure routing on the controller to use one of the following routing techniques:

- Static routes — Use static routes to set the default route of a controller so that legitimate wireless device traffic can be forwarded to the default gateway.
- OSPF (version 2) (RFC2328) — Use OSPF to allow the controller to participate in dynamic route selection. OSPF is a protocol designed for medium and large IP networks with the ability to segment



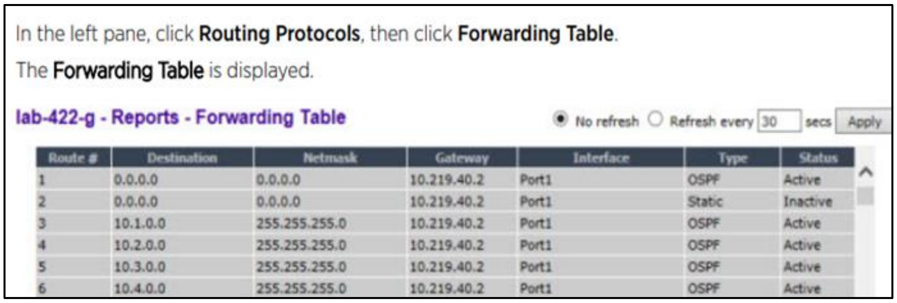
OSPF is an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately distributes the information to all other hosts in the network so that all will



OSPF

An interior gateway routing protocol for TCP/IP networks, Open Shortest Path First uses a link state routing algorithm that calculates routes for packets based on a number of factors, including least hops, speed of transmission lines, and congestion delays. You can also configure certain cost metrics for the algorithm. This protocol is more efficient and scalable than vector-distance routing protocols. OSPF features include least-cost routing, ECMP routing, and load balancing. Although OSPF requires CPU

[17]



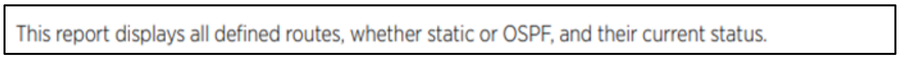
In the left pane, click **Routing Protocols**, then click **Forwarding Table**.

The **Forwarding Table** is displayed.

lab-422-g - Reports - Forwarding Table

● No refresh ○ Refresh every 30 secs

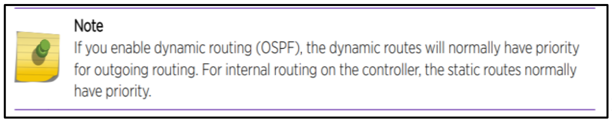
Route #	Destination	Netmask	Gateway	Interface	Type	Status
1	0.0.0.0	0.0.0.0	10.219.40.2	Port1	OSPF	Active
2	0.0.0.0	0.0.0.0	10.219.40.2	Port1	Static	Inactive
3	10.1.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
4	10.2.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
5	10.3.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
6	10.4.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active



This report displays all defined routes, whether static or OSPF, and their current status.

[16] https://emc.extremenetworks.com/content/oneview/docs/network/devices/docs/maps/l_ov_map_tab.htm#link.

[17] https://content.etilize.com/User-Manual/1044537499.pdf, page 275 of 708.

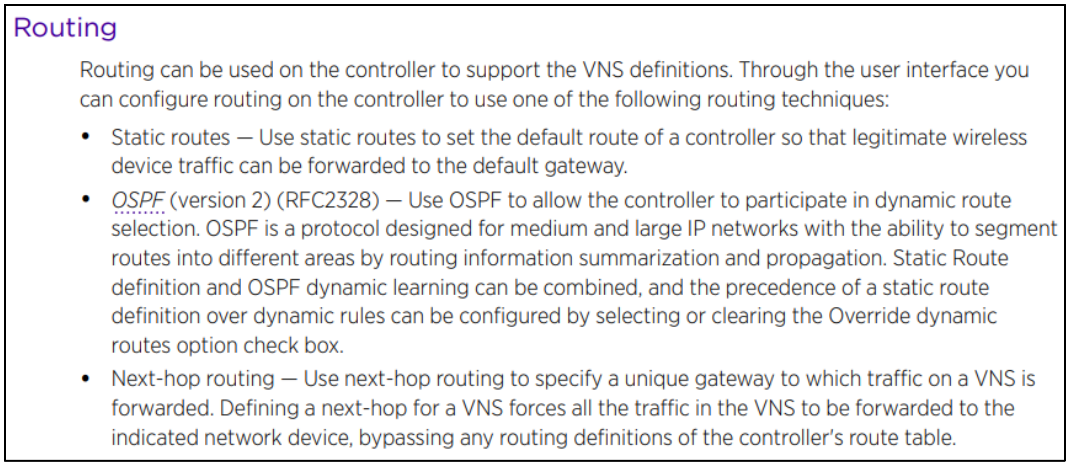


Note

If you enable dynamic routing (OSPF), the dynamic routes will normally have priority for outgoing routing. For internal routing on the controller, the static routes normally have priority.

[18]

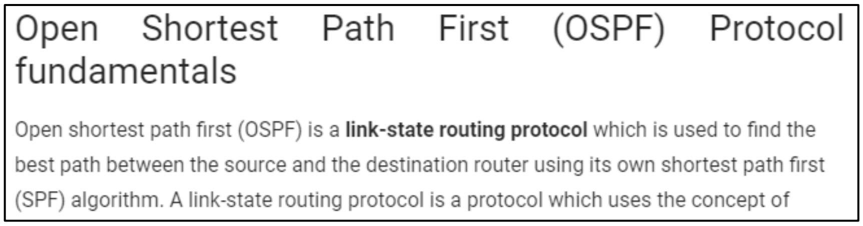
35. For example, the ExtremeWireless V10.41.01 performs the step of selecting a path from the plurality of paths in response to a first user input received via the GUI, wherein the selected path passes through two or more router nodes of the plurality of router nodes. Using the GUI, the user can select the unique gateway to which the traffic is forwarded. Or the user can select OSPF protocol which selects the best route when the user selects it using interface.



Routing

Routing can be used on the controller to support the VNS definitions. Through the user interface you can configure routing on the controller to use one of the following routing techniques:

- Static routes — Use static routes to set the default route of a controller so that legitimate wireless device traffic can be forwarded to the default gateway.
- OSPF (version 2) (RFC2328) — Use OSPF to allow the controller to participate in dynamic route selection. OSPF is a protocol designed for medium and large IP networks with the ability to segment routes into different areas by routing information summarization and propagation. Static Route definition and OSPF dynamic learning can be combined, and the precedence of a static route definition over dynamic rules can be configured by selecting or clearing the Override dynamic routes option check box.
- Next-hop routing — Use next-hop routing to specify a unique gateway to which traffic on a VNS is forwarded. Defining a next-hop for a VNS forces all the traffic in the VNS to be forwarded to the indicated network device, bypassing any routing definitions of the controller's route table.

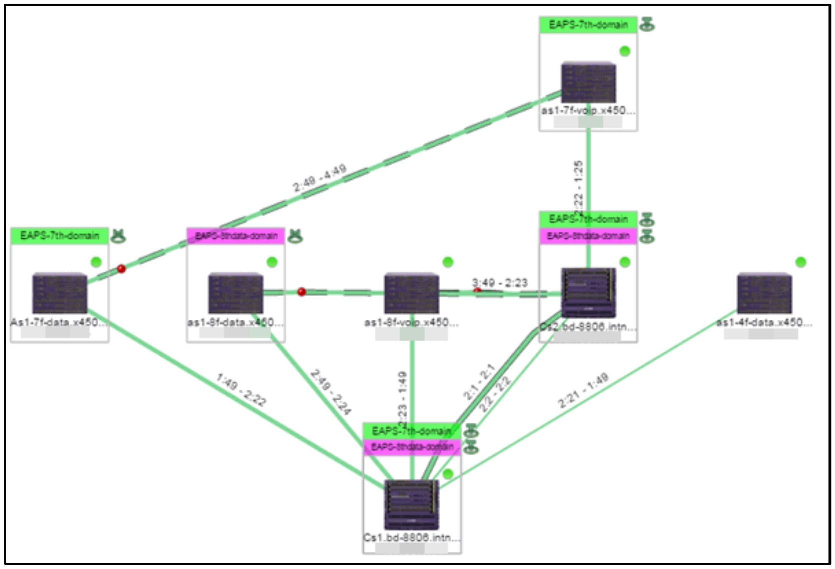


Open Shortest Path First (OSPF) Protocol fundamentals

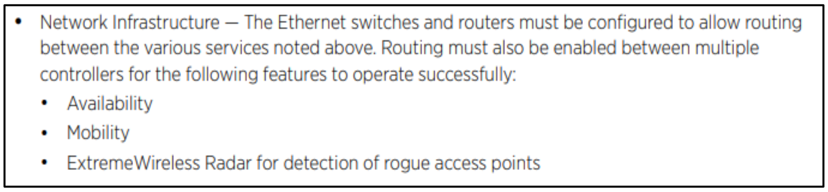
Open shortest path first (OSPF) is a **link-state routing protocol** which is used to find the best path between the source and the destination router using its own shortest path first (SPF) algorithm. A link-state routing protocol is a protocol which uses the concept of

[19]

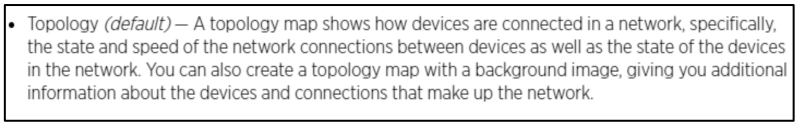
[18] https://content.etilize.com/User-Manual/1044537499.pdf , page 60, 61 of 708.
[19] https://www.geeksforgeeks.org/open-shortest-path-first-ospf-protocol-fundamentals/.



[20]

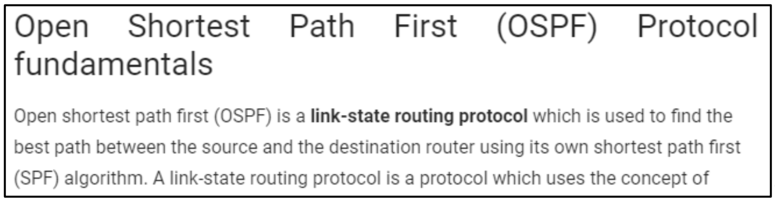


- Network Infrastructure — The Ethernet switches and routers must be configured to allow routing between the various services noted above. Routing must also be enabled between multiple controllers for the following features to operate successfully:
  - Availability
  - Mobility
  - ExtremeWireless Radar for detection of rogue access points



- Topology *(default)* — A topology map shows how devices are connected in a network, specifically, the state and speed of the network connections between devices as well as the state of the devices in the network. You can also create a topology map with a background image, giving you additional information about the devices and connections that make up the network.

[21]



Open Shortest Path First (OSPF) Protocol fundamentals

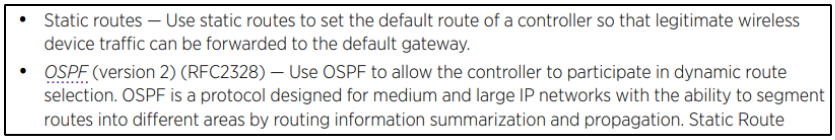
Open shortest path first (OSPF) is a **link-state routing protocol** which is used to find the best path between the source and the destination router using its own shortest path first (SPF) algorithm. A link-state routing protocol is a protocol which uses the concept of

[22]

[20] https://emc.extremenetworks.com/content/oneview/docs/network/devices/docs/maps/l_ov_map_tab.htm#link.

[21] https://content.etilize.com/User-Manual/1044537499.pdf, page 20 of 708.

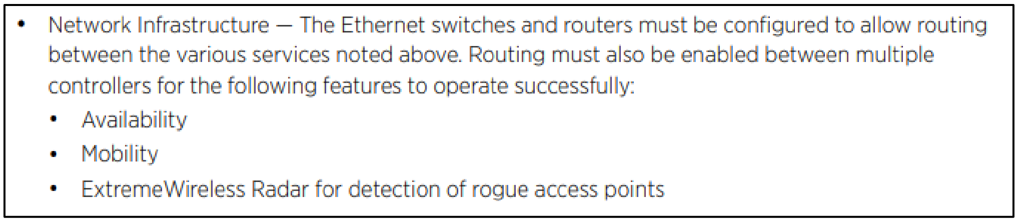
[22] https://www.geeksforgeeks.org/open-shortest-path-first-ospf-protocol-fundamentals/.



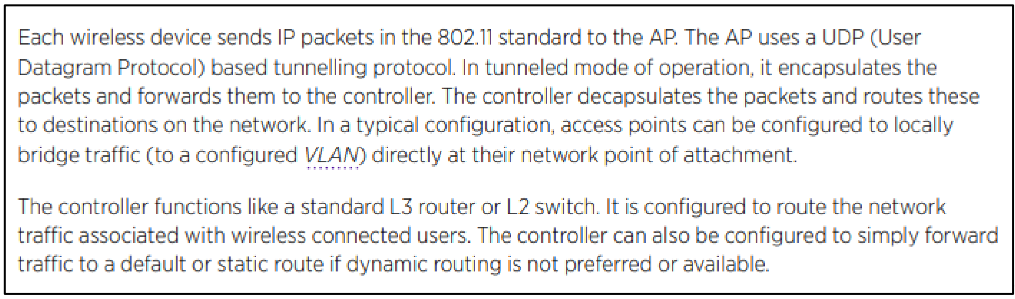
- Static routes — Use static routes to set the default route of a controller so that legitimate wireless device traffic can be forwarded to the default gateway.
- OSPF (version 2) (RFC2328) — Use OSPF to allow the controller to participate in dynamic route selection. OSPF is a protocol designed for medium and large IP networks with the ability to segment routes into different areas by routing information summarization and propagation. Static Route

[23]

36. For example, the ExtremeWireless V10.41.01 performs the step of initiating configuration of the two or more router nodes for communication between the first edge node and the second edge node in response to selecting the path.



- Network Infrastructure — The Ethernet switches and routers must be configured to allow routing between the various services noted above. Routing must also be enabled between multiple controllers for the following features to operate successfully:
  - Availability
  - Mobility
  - ExtremeWireless Radar for detection of rogue access points



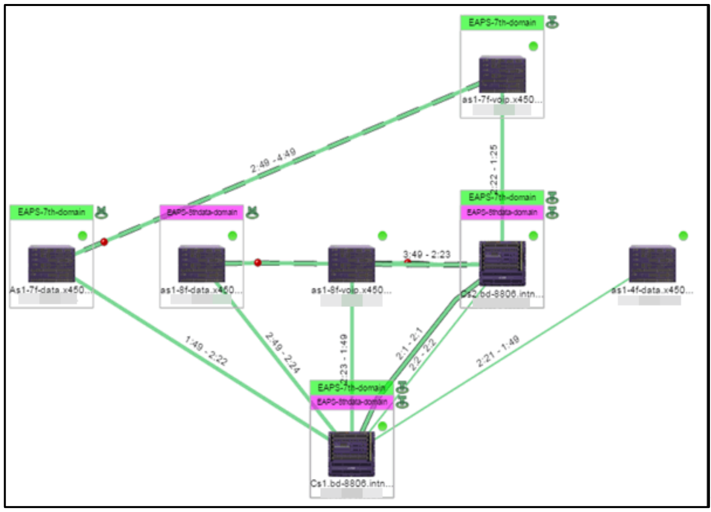
Each wireless device sends IP packets in the 802.11 standard to the AP. The AP uses a UDP (User Datagram Protocol) based tunnelling protocol. In tunneled mode of operation, it encapsulates the packets and forwards them to the controller. The controller decapsulates the packets and routes these to destinations on the network. In a typical configuration, access points can be configured to locally bridge traffic (to a configured VLAN) directly at their network point of attachment.

The controller functions like a standard L3 router or L2 switch. It is configured to route the network traffic associated with wireless connected users. The controller can also be configured to simply forward traffic to a default or static route if dynamic routing is not preferred or available.

[24]

[23] https://content.etilize.com/User-Manual/1044537499.pdf , page 28 of 708.

[24] https://content.etilize.com/User-Manual/1044537499.pdf , page 20, 21,23 of 708.



[25]

37. Defendant has and continues to indirectly infringe one or more claims of the ’646 Patent by knowingly and intentionally inducing others, including Extreme customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States infringing products.

38. Defendant, with knowledge that these products, or the use thereof, infringed the ’646 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’646 Patent by providing these products to end users for use in an infringing manner. Alternatively, on information and belief, Defendant has adopted a policy of not reviewing the patents of others, including specifically those related to Defendant’s specific industry, thereby remaining willfully blind to the Patent-in-Suit at least as early as the issuance of the Patents-in-Suit.

39. Defendant induced infringement by others, including end users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability

[25] https://emc.extremenetworks.com/content/oneview/docs/network/devices/docs/maps/l_ov_map_tab.htm#link.

that others, including end users, infringe the ’646 Patent, but while remaining willfully blind to the infringement. Defendant has and continues to induce infringement by its customers and end-users by supplying them with instructions on how to operate the Accused Instrumentalities in an infringing manner, while also making publicly available information on the Accused Instrumentalities via Defendant’s website and other publications. Upon information and belief, Defendant provides product support to its customers and end-users, where Defendant further instructs them to use the Accused Instrumentalities in an infringing manner.

40. Winterspring has suffered damages as a result of Defendant’s direct and indirect infringement of the ’646 Patent in an amount to be proved at trial.

41. Winterspring has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’646 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

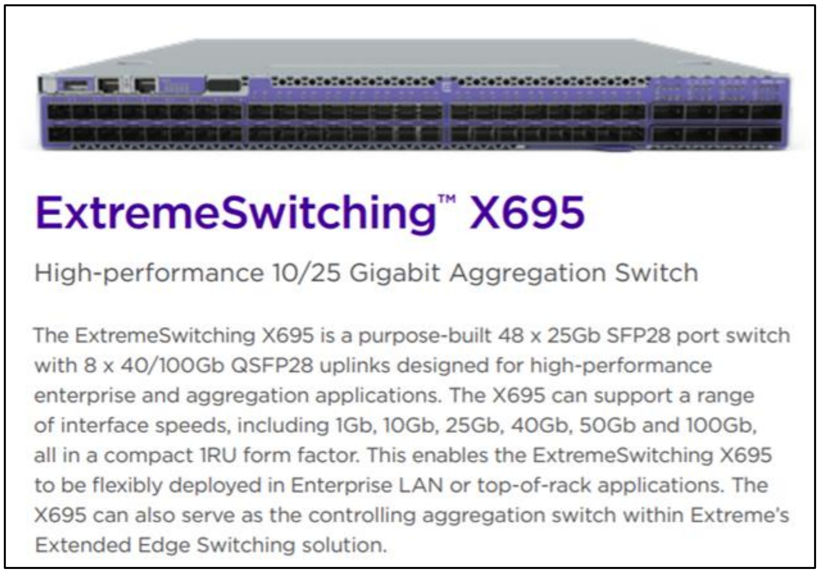
COUNT III
(Infringement of the ’975 Patent)

42. Paragraphs 1 through 13 are incorporated by reference as if fully set forth herein.

43. Winterspring has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the ’975 Patent.

44. Defendant has and continues to directly infringe the ’975 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’975 Patent. Such products include, but are not limited to, computers, network switches, modules, and software that perform packet tagging.

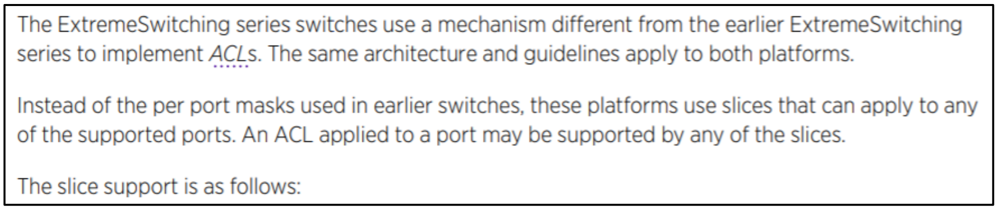
45. For example, Defendant has and continues to directly infringe at least claim 5 of the ’975 Patent by making, using, offering to sell, selling, and/or importing into the United States products that perform packet tagging, such as the ExtremeSwitching X695.



ExtremeSwitching™ X695

High-performance 10/25 Gigabit Aggregation Switch

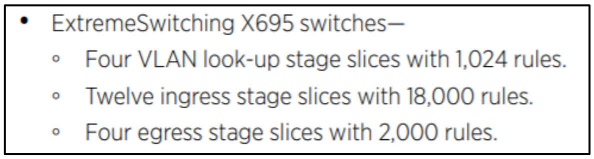
The ExtremeSwitching X695 is a purpose-built 48 x 25Gb SFP28 port switch with 8 x 40/100Gb QSFP28 uplinks designed for high-performance enterprise and aggregation applications. The X695 can support a range of interface speeds, including 1Gb, 10Gb, 25Gb, 40Gb, 50Gb and 100Gb, all in a compact 1RU form factor. This enables the ExtremeSwitching X695 to be flexibly deployed in Enterprise LAN or top-of-rack applications. The X695 can also serve as the controlling aggregation switch within Extreme's Extended Edge Switching solution.[26]



The ExtremeSwitching series switches use a mechanism different from the earlier ExtremeSwitching series to implement ACLs. The same architecture and guidelines apply to both platforms.

Instead of the per port masks used in earlier switches, these platforms use slices that can apply to any of the supported ports. An ACL applied to a port may be supported by any of the slices.

The slice support is as follows:



- ExtremeSwitching X695 switches—
  - Four VLAN look-up stage slices with 1,024 rules.
  - Twelve ingress stage slices with 18,000 rules.
  - Four egress stage slices with 2,000 rules.

[27]

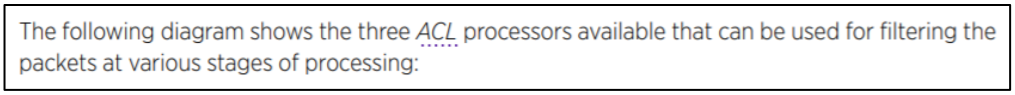
46. For example, the ExtremeSwitching X695 includes an apparatus comprising a network processor interface suitable for coupling to a network processor and a central processor

[26] https://cloud.kapostcontent.net/pub/0369b53f-0179-40bb-b364-81a84d8354ce/x695-data-sheet, Page 1/8.

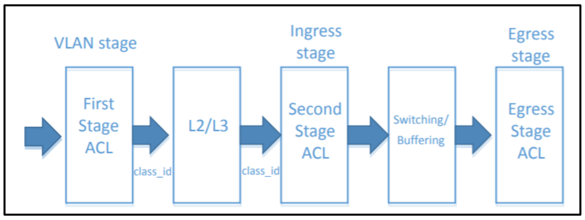
[27] https://documentation.extremenetworks.com/exos_30.6/downloads/EXOS_User_Guide_30_6.pdf, Page 755 and 756/2089.

interface suitable for coupling to a central processor. The ingress processor is the network processor.

Two-Stage ACL



The following diagram shows the three ACL processors available that can be used for filtering the packets at various stages of processing:



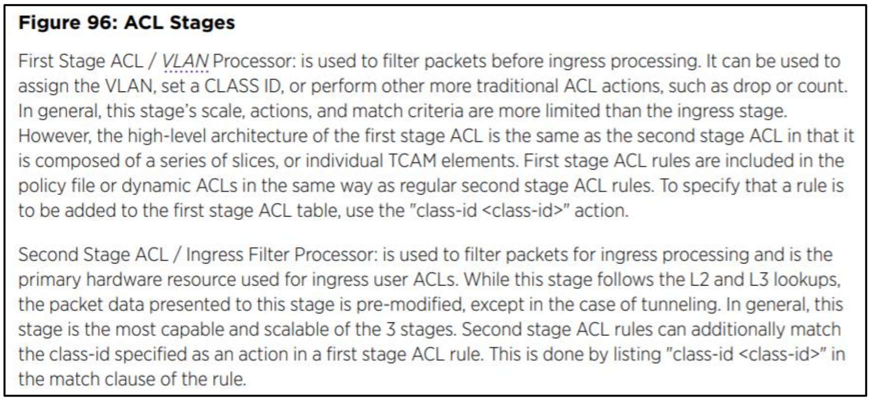


Figure 96: ACL Stages

First Stage ACL / VLAN Processor: is used to filter packets before ingress processing. It can be used to assign the VLAN, set a CLASS ID, or perform other more traditional ACL actions, such as drop or count. In general, this stage's scale, actions, and match criteria are more limited than the ingress stage. However, the high-level architecture of the first stage ACL is the same as the second stage ACL in that it is composed of a series of slices, or individual TCAM elements. First stage ACL rules are included in the policy file or dynamic ACLs in the same way as regular second stage ACL rules. To specify that a rule is to be added to the first stage ACL table, use the "class-id <class-id>" action.

Second Stage ACL / Ingress Filter Processor: is used to filter packets for ingress processing and is the primary hardware resource used for ingress user ACLs. While this stage follows the L2 and L3 lookups, the packet data presented to this stage is pre-modified, except in the case of tunneling. In general, this stage is the most capable and scalable of the 3 stages. Second stage ACL rules can additionally match the class-id specified as an action in a first stage ACL rule. This is done by listing "class-id <class-id>" in the match clause of the rule.

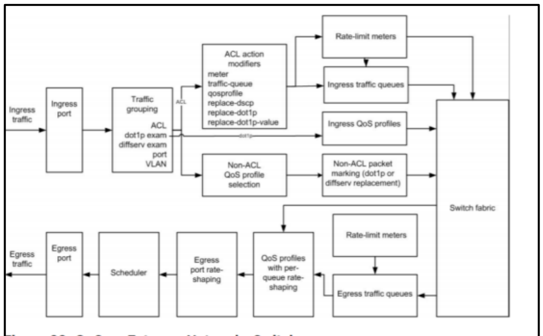
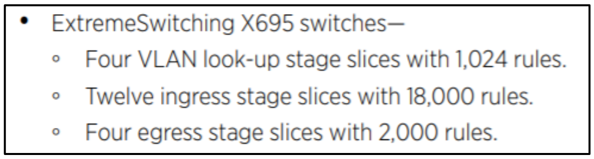


Figure 99: QoS on Extreme Networks Switches [28]

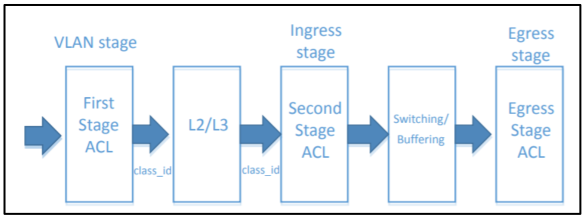
[28] https://documentation.extremenetworks.com/exos_30.6/downloads/EXOS_User_Guide_30_6.pdf Page 789/2089.

47. For example, the ExtremeSwitching X695 comprises a protocol determination logic block to determine a protocol type of data in a packet, wherein the protocol determination logic compares the protocol information in a first pass to predetermined values to procedure a first result and, if the first result is positive, compares the protocol information in a second pass to predetermined values to produce a second result, the first and second results forming a set of results. The First Stage ACL/VLAN processor is the protocol determination logic block. The First Stage ACL/VLAN processor is the protocol determination logic block. It determines the protocol type of the incoming packet based on the 802.1q tag or the protocol type of the packet.



- ExtremeSwitching X695 switches—
  - Four VLAN look-up stage slices with 1,024 rules.
  - Twelve ingress stage slices with 18,000 rules.
  - Four egress stage slices with 2,000 rules.

[29]



[29] https://documentation.extremenetworks.com/exos_30.6/downloads/EXOS_User_Guide_30_6.pdf Page 756/2089.

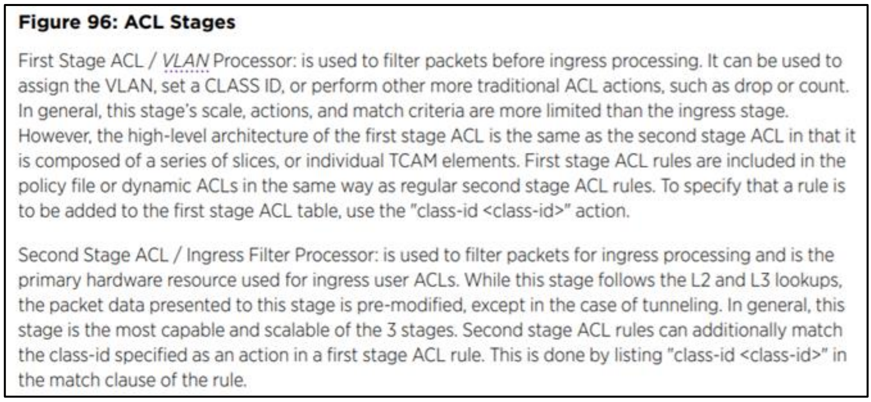
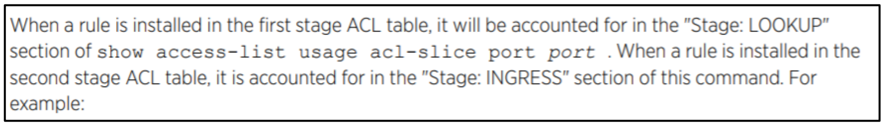


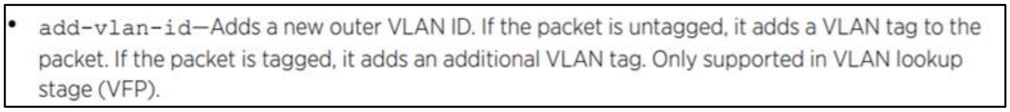
Figure 96: ACL Stages

First Stage ACL / VLAN Processor: is used to filter packets before ingress processing. It can be used to assign the VLAN, set a CLASS ID, or perform other more traditional ACL actions, such as drop or count. In general, this stage's scale, actions, and match criteria are more limited than the ingress stage. However, the high-level architecture of the first stage ACL is the same as the second stage ACL in that it is composed of a series of slices, or individual TCAM elements. First stage ACL rules are included in the policy file or dynamic ACLs in the same way as regular second stage ACL rules. To specify that a rule is to be added to the first stage ACL table, use the "class-id <class-id>" action.

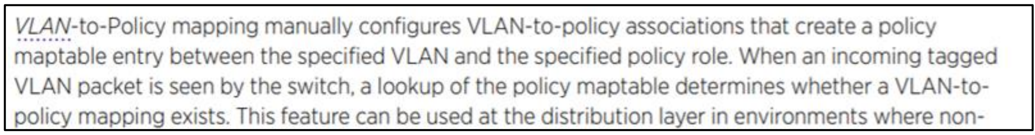
Second Stage ACL / Ingress Filter Processor: is used to filter packets for ingress processing and is the primary hardware resource used for ingress user ACLs. While this stage follows the L2 and L3 lookups, the packet data presented to this stage is pre-modified, except in the case of tunneling. In general, this stage is the most capable and scalable of the 3 stages. Second stage ACL rules can additionally match the class-id specified as an action in a first stage ACL rule. This is done by listing "class-id <class-id>" in the match clause of the rule.[30]



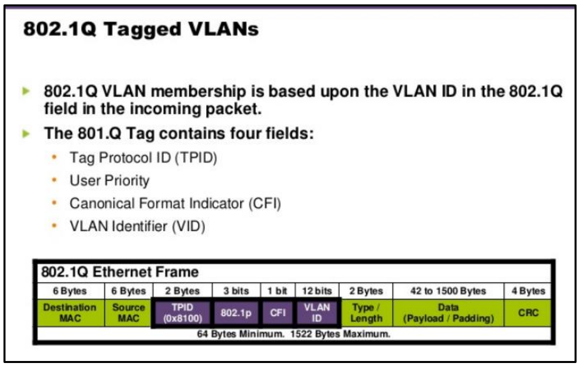
When a rule is installed in the first stage ACL table, it will be accounted for in the "Stage: LOOKUP" section of `show access-list usage acl-slice port` *`port`* . When a rule is installed in the second stage ACL table, it is accounted for in the "Stage: INGRESS" section of this command. For example:[31]



- `add-vlan-id`—Adds a new outer VLAN ID. If the packet is untagged, it adds a VLAN tag to the packet. If the packet is tagged, it adds an additional VLAN tag. Only supported in VLAN lookup stage (VFP).[32]



VLAN-to-Policy mapping manually configures VLAN-to-policy associations that create a policy maptable entry between the specified VLAN and the specified policy role. When an incoming tagged VLAN packet is seen by the switch, a lookup of the policy maptable determines whether a VLAN-to-policy mapping exists. This feature can be used at the distribution layer in environments where non-[33]



802.1Q Tagged VLANs

- **802.1Q VLAN membership is based upon the VLAN ID in the 802.1Q field in the incoming packet.**
- **The 801.Q Tag contains four fields:**
  - Tag Protocol ID (TPID)
  - User Priority
  - Canonical Format Indicator (CFI)
  - VLAN Identifier (VID)

802.1Q Ethernet Frame

6 Bytes	6 Bytes	2 Bytes	3 bits	1 bit	12 bits	2 Bytes	42 to 1500 Bytes	4 Bytes
Destination MAC	Source MAC	TPID (0x8100)	802.1p	CFI	VLAN ID	Type / Length	Data (Payload / Padding)	CRC

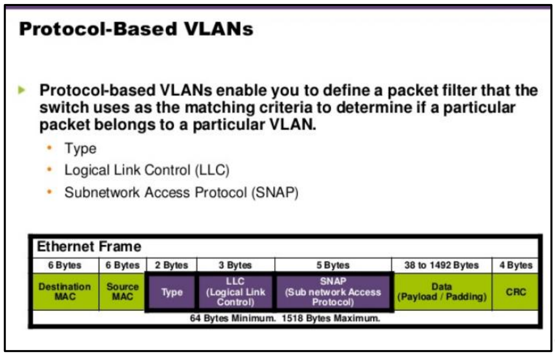
64 Bytes Minimum. 1522 Bytes Maximum.

[30] https://documentation.extremenetworks.com/exos_30.6/downloads/EXOS_User_Guide_30_6.pdf Page 710, 711/2089.

[31] https://documentation.extremenetworks.com, Page 712/2089.

[32] https://documentation.extremenetworks.com Page 719/2089.

[33] https://documentation.extremenetworks.com/exos_30.6/ Page 878/2089.



Protocol-Based VLANs

- **Protocol-based VLANs enable you to define a packet filter that the switch uses as the matching criteria to determine if a particular packet belongs to a particular VLAN.**
  - Type
  - Logical Link Control (LLC)
  - Subnetwork Access Protocol (SNAP)

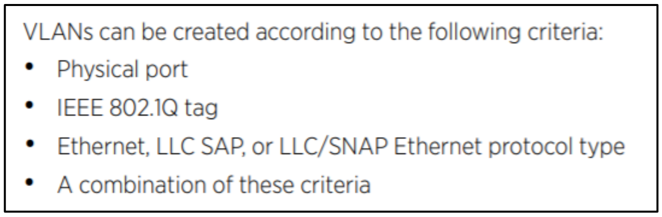
Ethernet Frame

6 Bytes	6 Bytes	2 Bytes	3 Bytes	5 Bytes	38 to 1492 Bytes	4 Bytes
Destination MAC	Source MAC	Type	LLC (Logical Link Control)	SNAP (Sub network Access Protocol)	Data (Payload / Padding)	CRC

64 Bytes Minimum. 1518 Bytes Maximum.

[34]

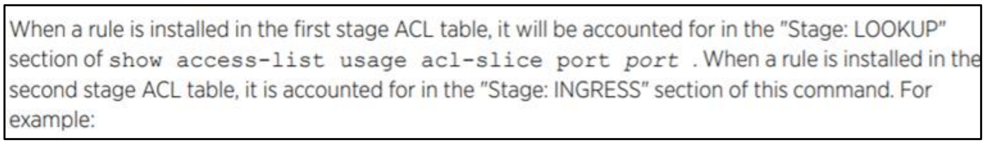
48. If the tagged packet is determined, the ACL also checks for the matching conditions (second pass). Based on the type of packet and the ACL filtering (set of results), the packet is allowed.



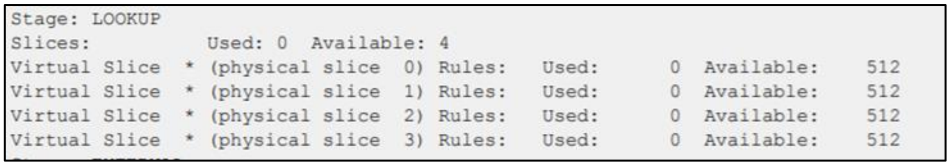
VLANs can be created according to the following criteria:

- Physical port
- IEEE 802.1Q tag
- Ethernet, LLC SAP, or LLC/SNAP Ethernet protocol type
- A combination of these criteria

[35]



When a rule is installed in the first stage ACL table, it will be accounted for in the "Stage: LOOKUP" section of `show access-list usage acl-slice port` *`port`* . When a rule is installed in the second stage ACL table, it is accounted for in the "Stage: INGRESS" section of this command. For example:



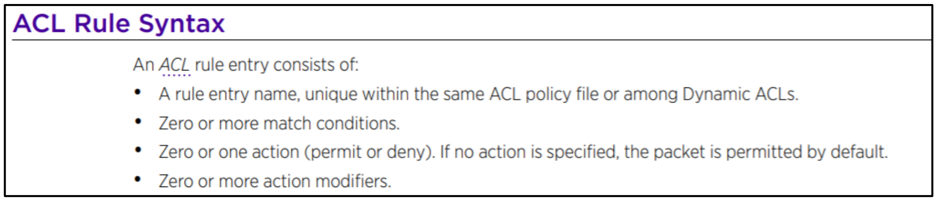
```
Stage: LOOKUP
Slices:            Used: 0   Available: 4
Virtual Slice  * (physical slice  0) Rules:   Used:      0  Available:    512
Virtual Slice  * (physical slice  1) Rules:   Used:      0  Available:    512
Virtual Slice  * (physical slice  2) Rules:   Used:      0  Available:    512
Virtual Slice  * (physical slice  3) Rules:   Used:      0  Available:    512
```

[36]

[34] https://www.slideshare.net/simanjuntakdani/vlan-network-for-extreme-networks Slide 7 and 9/51.

[35] https://documentation.extremenetworks.com/exos_30.6/downloads/EXOS_User_Guide_30_6.pdf Page 543/2089.

[36] https://documentation.extremenetworks.com/exos_30.6/ Page 712/2089.

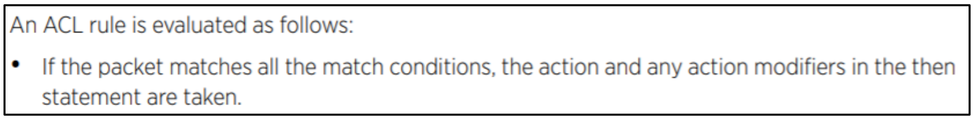


ACL Rule Syntax

An ACL rule entry consists of:

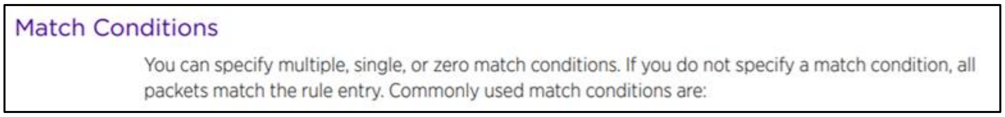
- A rule entry name, unique within the same ACL policy file or among Dynamic ACLs.
- Zero or more match conditions.
- Zero or one action (permit or deny). If no action is specified, the packet is permitted by default.
- Zero or more action modifiers.

[37]



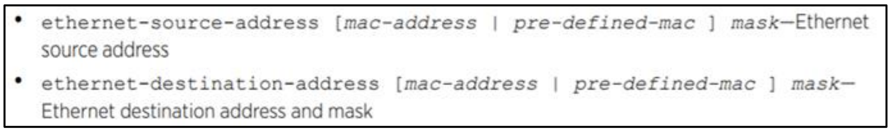
An ACL rule is evaluated as follows:

- If the packet matches all the match conditions, the action and any action modifiers in the then statement are taken.

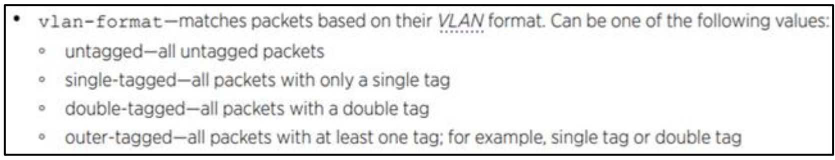


Match Conditions

You can specify multiple, single, or zero match conditions. If you do not specify a match condition, all packets match the rule entry. Commonly used match conditions are:



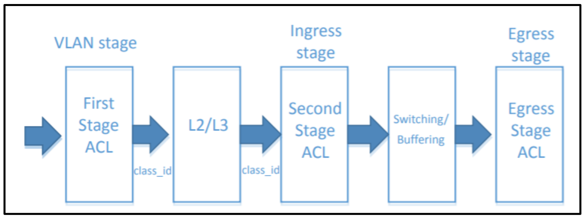
- `ethernet-source-address [mac-address | pre-defined-mac ] mask`—Ethernet source address
- `ethernet-destination-address [mac-address | pre-defined-mac ] mask`—Ethernet destination address and mask



- `vlan-format`—matches packets based on their VLAN format. Can be one of the following values:
  - untagged—all untagged packets
  - single-tagged—all packets with only a single tag
  - double-tagged—all packets with a double tag
  - outer-tagged—all packets with at least one tag; for example, single tag or double tag

[38]

49. If the packet is untagged (first result negative), the VLAN processor (tag select logic) adds a VLAN tag to the packet.



[37] https://documentation.extremenetworks.com Page 714/2089.

[38] https://documentation.extremenetworks.com/exos_30.6/ Page 715 and 717/2089.

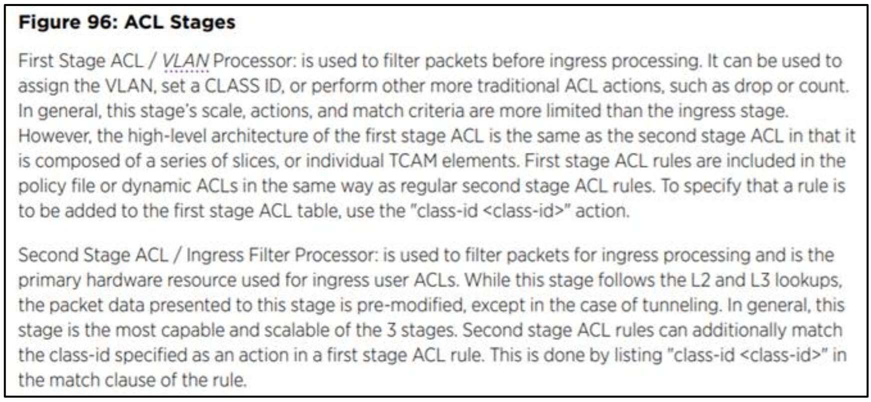
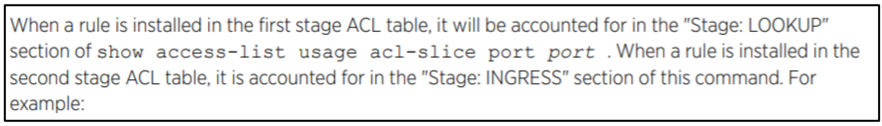


Figure 96: ACL Stages

First Stage ACL / VLAN Processor: is used to filter packets before ingress processing. It can be used to assign the VLAN, set a CLASS ID, or perform other more traditional ACL actions, such as drop or count. In general, this stage's scale, actions, and match criteria are more limited than the ingress stage. However, the high-level architecture of the first stage ACL is the same as the second stage ACL in that it is composed of a series of slices, or individual TCAM elements. First stage ACL rules are included in the policy file or dynamic ACLs in the same way as regular second stage ACL rules. To specify that a rule is to be added to the first stage ACL table, use the "class-id <class-id>" action.

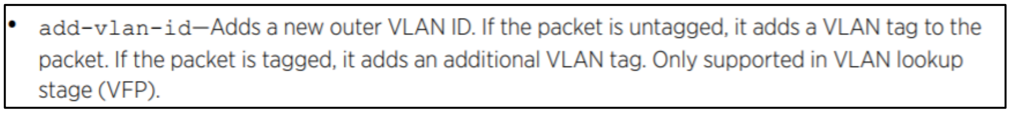
Second Stage ACL / Ingress Filter Processor: is used to filter packets for ingress processing and is the primary hardware resource used for ingress user ACLs. While this stage follows the L2 and L3 lookups, the packet data presented to this stage is pre-modified, except in the case of tunneling. In general, this stage is the most capable and scalable of the 3 stages. Second stage ACL rules can additionally match the class-id specified as an action in a first stage ACL rule. This is done by listing "class-id <class-id>" in the match clause of the rule.

[39]



When a rule is installed in the first stage ACL table, it will be accounted for in the "Stage: LOOKUP" section of `show access-list usage acl-slice port` *`port`* . When a rule is installed in the second stage ACL table, it is accounted for in the "Stage: INGRESS" section of this command. For example:

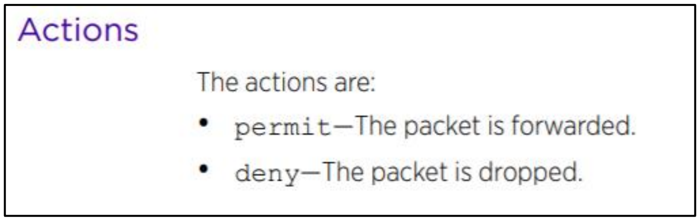
[40]



- `add-vlan-id`—Adds a new outer VLAN ID. If the packet is untagged, it adds a VLAN tag to the packet. If the packet is tagged, it adds an additional VLAN tag. Only supported in VLAN lookup stage (VFP).

[41]

50. If the tagged packet is determined, the ACL also checks for the matching conditions (second pass). Based on the type of packet and the ACL filtering (set of results), the packet is forwarded to the Ingress processor (network processor interface).



Actions

The actions are:

- `permit`—The packet is forwarded.
- `deny`—The packet is dropped.

[42]

[39] https://documentation.extremenetworks.com/exos_30.6/downloads/EXOS_User_Guide_30_6.pdf Page 710, 711/2089.

[40] https://documentation.extremenetworks.com Page 712/2089.

[41] https://documentation.extremenetworks.com Page 719/2089.

[42] https://documentation.extremenetworks.com Page 715/2089.

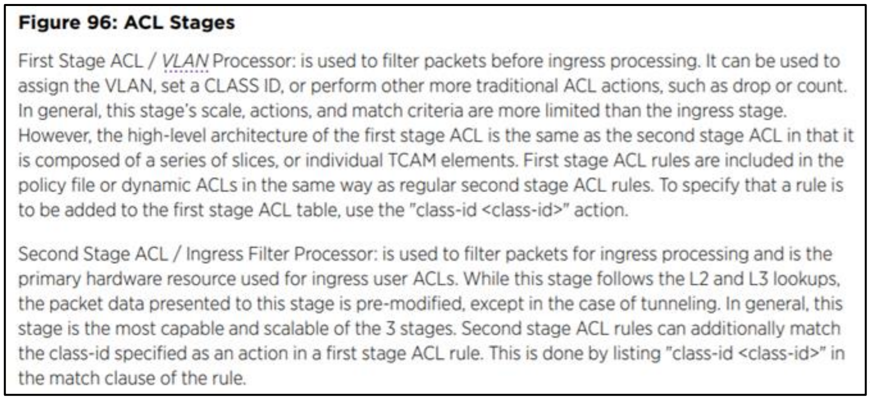
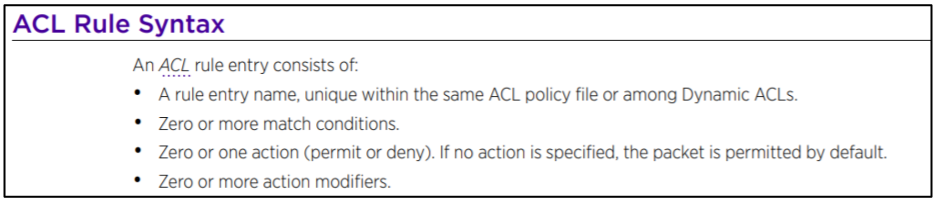


Figure 96: ACL Stages

First Stage ACL / VLAN Processor: is used to filter packets before ingress processing. It can be used to assign the VLAN, set a CLASS ID, or perform other more traditional ACL actions, such as drop or count. In general, this stage's scale, actions, and match criteria are more limited than the ingress stage. However, the high-level architecture of the first stage ACL is the same as the second stage ACL in that it is composed of a series of slices, or individual TCAM elements. First stage ACL rules are included in the policy file or dynamic ACLs in the same way as regular second stage ACL rules. To specify that a rule is to be added to the first stage ACL table, use the "class-id <class-id>" action.

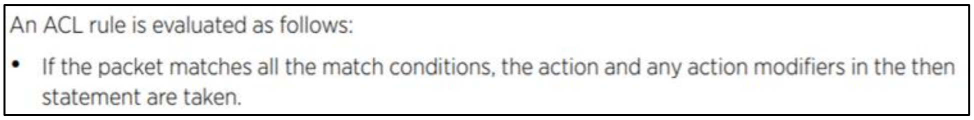
Second Stage ACL / Ingress Filter Processor: is used to filter packets for ingress processing and is the primary hardware resource used for ingress user ACLs. While this stage follows the L2 and L3 lookups, the packet data presented to this stage is pre-modified, except in the case of tunneling. In general, this stage is the most capable and scalable of the 3 stages. Second stage ACL rules can additionally match the class-id specified as an action in a first stage ACL rule. This is done by listing "class-id <class-id>" in the match clause of the rule. [43]



ACL Rule Syntax

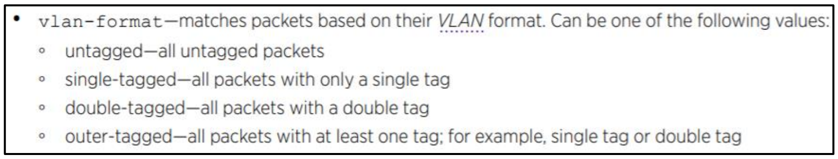
An ACL rule entry consists of:

- A rule entry name, unique within the same ACL policy file or among Dynamic ACLs.
- Zero or more match conditions.
- Zero or one action (permit or deny). If no action is specified, the packet is permitted by default.
- Zero or more action modifiers.



An ACL rule is evaluated as follows:

- If the packet matches all the match conditions, the action and any action modifiers in the then statement are taken.



- `vlan-format`—matches packets based on their VLAN format. Can be one of the following values:
  - untagged—all untagged packets
  - single-tagged—all packets with only a single tag
  - double-tagged—all packets with a double tag
  - outer-tagged—all packets with at least one tag; for example, single tag or double tag

[44]

51. Defendant has and continues to indirectly infringe one or more claims of the ’975 Patent by knowingly and intentionally inducing others, including Extreme customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States infringing products.

52. Defendant, with knowledge that these products, or the use thereof, infringed the ’975 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and

[43] https://documentation.extremenetworks.com/exos_30.6/downloads/EXOS_User_Guide_30_6.pdf Page 710, 711/2089.

[44] https://documentation.extremenetworks.com Page 714, 715 and 717/2089.

continues to knowingly and intentionally induce, direct infringement of the ’975 Patent by providing these products to end users for use in an infringing manner. Alternatively, on information and belief, Defendant has adopted a policy of not reviewing the patents of others, including specifically those related to Defendant’s specific industry, thereby remaining willfully blind to the Patent-in-Suit at least as early as the issuance of the Patents-in-Suit.

53. Defendant induced infringement by others, including end users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end users, infringe the ’975 Patent, but while remaining willfully blind to the infringement. Defendant has and continues to induce infringement by its customers and end-users by supplying them with instructions on how to operate the Accused Instrumentalities in an infringing manner, while also making publicly available information on the Accused Instrumentalities via Defendant’s website and other publications. Upon information and belief, Defendant provides product support to its customers and end-users, where Defendant further instructs them to use the Accused Instrumentalities in an infringing manner.

54. Winterspring has suffered damages as a result of Defendant’s direct and indirect infringement of the ’975 Patent in an amount to be proved at trial.

55. Winterspring has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’975 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury for all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Winterspring prays for relief against Defendant as follows:

a. Entry of judgment declaring that Defendant has directly and/or indirectly infringed one or more claims of the Patents-in-Suit;

b. An order pursuant to 35 U.S.C. § 283 permanently enjoining Defendant, its officers, agents, servants, employees, attorneys, and those persons in active concert or participation with it, from further acts of infringement of one or more of the Patents-in-Suit;

c. An order awarding damages sufficient to compensate Winterspring for Defendant's infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, together with interest and costs;

d. Entry of judgment declaring that this case is exceptional and awarding Winterspring its costs and reasonable attorney fees under 35 U.S.C. § 285; and,

e. Such other and further relief as the Court deems just and proper.

Dated: August 21, 2023

Respectfully submitted,

/s/ Vincent J. Rubino, III
Alfred R. Fabricant
NY Bar No. 2219392
Email: ffabricant@fabricantllp.com
Peter Lambrianakos
NY Bar No. 2894392
Email: plambrianakos@fabricantllp.com
Vincent J. Rubino, III
NY Bar No. 4557435
Email: vrubino@fabricantllp.com
FABRICANT LLP
411 Theodore Fremd Road, Suite 206 South
Rye, NY 10580
Telephone: (212) 257-5797
Facsimile: (212) 257-5796

Justin Kurt Truelove
Texas Bar No. 24013653
Email: kurt@truelovelawfirm.com
TRUELOVE LAW FIRM, PLLC
100 West Houston
Marshall, Texas 75670

Telephone: (903) 938-8321
Facsimile: (903) 215-8510

ATTORNEYS FOR PLAINTIFF
WINTERSPRING DIGITAL LLC