ExtremeSwitching™

Release Notes for VOSS

Release 8.0 (VOSS)
9035640 Rev.03
June 2019

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: www.extremenetworks.com/support/policies/software-licensing

Contents

Chapter 1: About this Document

Purpose

This document describes important information about this release for supported VSP Operating System Software (VOSS) platforms.

This document includes the following information:

- supported hardware and software
- scaling capabilities
- known issues, including workarounds where appropriate
- known restrictions

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that can be used throughout this document.

Table 1: Notice Icons

Icon	Alerts you to...
Important:	A situation that can cause serious inconvenience.
Note:	Important features or instructions.
Tip:	Helpful tips and notices for using the product.
Danger:	Situations that will result in severe bodily injury; up to and including death.
Warning:	Risk of severe personal injury or critical loss of data.

Table continues…

Icon	Alerts you to...
⚠ **Caution:**	Risk of personal injury, system damage, or loss of data.

Table 2: Text Conventions

Convention	Description
Angle brackets (< >)	Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. If the command syntax is `cfm maintenance-domain maintenance-level <0-7>` , you can enter `cfm maintenance-domain maintenance-level 4`.
Bold text	Bold text indicates the GUI object name you must act upon. Examples: • Click **OK**. • On the **Tools** menu, choose **Options**.
Braces ({ })	Braces ({ }) indicate required elements in syntax descriptions. Do not type the braces when you enter the command. For example, if the command syntax is `ip address {A.B.C.D}`, you must enter the IP address in dotted, decimal notation.
Brackets ([ ])	Brackets ([ ]) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command. For example, if the command syntax is `show clock [detail]`, you can enter either `show clock` or `show clock detail`.
Ellipses (…)	An ellipsis (…) indicates that you repeat the last element of the command as needed. For example, if the command syntax is `ethernet/2/1 [ <parameter> <value> ]...`, you enter `ethernet/2/1` and as many parameter-value pairs as you need.
Italic Text	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.

Table continues…

Convention	Description
`Plain Courier Text`	Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages. Examples: • `show ip route` • `Error: Invalid command syntax [Failed][2013-03-22 13:37:03.303 -04:00]`
Separator (>)	A greater than sign (>) shows separation in menu paths. For example, in the Navigation tree, expand the **Configuration** > **Edit** folders.
Vertical Line (|)	A vertical line (|) separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command. For example, if the command syntax is `access-policy by-mac action { allow | deny }`, you enter either `access-policy by-mac action allow` or `access-policy by-mac action deny`, but not both.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
The Hub	A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
Call GTAC	For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form with your information (all fields are required).
3. Select the products for which you would like to receive notifications.

   Note:
   You can modify your product selections or unsubscribe at any time.
4. Click **Submit**.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Chapter 2: New in this Release

The following sections describe what is new in VOSS 8.0. For a full list of features, see Features by Release on page 99.

Important:

The following platforms support VOSS 8.0:

- VSP 4450 Series
- VSP 7200 Series
- VSP 7400 Series
- VSP 8000 Series, which includes VSP 8200 Series and VSP 8400 Series

New Hardware

VSP 7432CQ

VOSS 8.0 adds support for a new hardware model that provides 32 ports of 100 Gbps Ethernet, optimized for the core and aggregation layers. The ports have a QSFP form factor and accept either QSFP+ (40 Gbps) or QSFP28 (100 Gbps) transceivers.

The transceiver type used in a port determines the port speed as either 100 Gbps for QSFP28 or 40 Gbps for QSFP+. This detection is dynamic and requires no software configuration. When channelization is enabled on a port, the sub-port speed is automatically determined based on the type of transceiver inserted, for example, 4x25 Gbps sub-ports for QSFP28 or 4x10 Gbps ports for QSFP+.

You can channelize 31 of the 32 ports; you cannot channelize port 28. Because the switch supports QSFP28 or QSFP+ transceivers and channelization, the ports can operate at the following speeds:

- 100 Gbps
- 4 x 25 Gbps (when channelization is enabled)
- 40 Gbps
- 4 x 10 Gbps (when channelization is enabled)

For more information, see VSP 7400 Series Switches: Hardware Installation Guide.

Transceivers

VOSS 8.0 introduces support for the following transceivers and direct attach cables:

- 10 Gbps pluggables:
  - 10 Gb Bidirectional 10 km SFP+ Module (PN: 10GB-BX10-D, 10GB-BX10- U)
- 25 Gbps pluggables, when used with QSFP28 to SFP28 Adapter (PN: 10506) on VSP 7432CQ and channelization:
  - 25 Gb SR SFP28 (PN: 10501)
  - 25 Gb SR-Lite MMF (Multimode Fiber) SFP28 (PN: 10502)
  - 25 Gb ESR SFP28 (PN: 10503)
  - 25 Gb LR 10 km SFP28 (PN: 10504)
  - Cables:

Description	Model Number	Length
25 Gb, SFP28-SFP28 passive copper cable	10520	1 meter
	10521	3 meter
	10522	5 meter
25 Gb, SFP28-SFP28 active optical cable	10530	10 meter
	10531	20 meter

- 40 Gbps pluggables:
  - 40 Gb SR4 QSFP+ (PN: 10319)
  - 40 Gb LM4 QSFP+ (PN: 10334)
- 100 Gbps pluggables:
  - 100 Gb PSM4 (Parallel Single-Mode) QSFP28 (PN: 10405)
  - Cables:

Description	Model Number	Length
100 Gb, QSFP28-4xSFP28 (4x25Gb) passive copper breakout cable	10421	1 meter
	10423	3 meter
	10424	5 meter
100 Gb, QSFP28-4xSFP28 (4x25Gb) active optical breakout cable	10444	20 meter

The following table indicates where to find more information about optical transceivers and components.

Extreme Networks optical transceivers and components	*Extreme Networks Pluggable Transceivers Installation Guide*

Table continues…

Compatibility for Extreme Networks SFP, SFP+, QSFP+, and QSFP28 transceiver modules with the VSP series switches	VSP Components: SFP, SFP+, QSFP+, QSFP28 Support

VOSS 8.0

Advanced Feature Bandwidth Reservation

The **`advanced-feature-bandwidth-reservation`** boot flag enables you to either use all ports on the switch or to reserve ports as loopback ports (default) to support advanced features, such as Fabric Extend, SPB, SMLT, vIST, VXLAN Gateway, Fabric RSPAN (Mirror to I-SID), Application Telemetry, or IS-IS Accept Policies.

This feature is specific to VSP 7400 Series.

For more information, see Administering VOSS.

Application Telemetry enhancements

Application Telemetry is enhanced to support interaction with Analytics Engine on either an external server or on-switch virtual machine. Application Telemetry and sFlow collector configuration has been enhanced to include reachability status.

For more information, see Monitoring Performance for VOSS.

Extreme Insight

Extreme Insight Architecture provides a flexible and open solution that enables organizations to deploy high-performance and flexible visibility applications pervasively throughout their network for improved monitoring and troubleshooting. Enabled by the Extreme VSP Operating System Software (VOSS), this preconfigured QEMU/KVM environment leverages high performance x86 CPUs to host these applications, extending visibility customized to the business and operational needs of the organization across the entire network.

The Extreme Insight Architecture open QEMU/KVM environment supports several pretested and well-known packet capture applications in a Linux virtual machine, including Wireshark and tcpdump. There are a wide variety of additional applications, tools, and utilities that organizations are able to run in this environment, such as data analytics applications, packet generators, monitoring tools, troubleshooting utilities, and many others. While the QEMU/KVM environment is open and can host any application, it is designed and ideally suited for networking applications, tools, and utilities. It also supports ExtremeAnalytics virtual engine that captures and analyzes context-based application information to deliver business insights on applications, users, locations and devices. By providing dedicated resources on the router or switch, organizations can gain unparalleled insight into the network through pervasive low-latency capture of real-time visibility traffic without impacting the normal control and forwarding of the network.

A key benefit of the Extreme Insight Architecture is to enable organizations to deploy high-performance and flexible visibility applications via dedicated resources on the platform, including:

- Dedicated internal and external bandwidth that allows applications running in the open QEMU/KVM environment to extract data without disrupting forwarding or control plane traffic and to deliver the captured data to analytics applications off the platform.

- Dedicated industry-standard x86 CPUs.

This feature is specific to VSP 7400 Series.

For more information, see Configuring User Interfaces and Operating Systems for VOSS.

Forward Error Correction (FEC)

This release introduces support for the configuration of Forward Error Correction (FEC) on the 100 Gbps ports of the VSP 7400 Series and VSP 8400 Series. This release also supports an automatic configuration option, which configures FEC based on port speed and pluggable module type. FEC is used for enhanced error correction when transmitting data over a noisy channel.

Note:

FEC is not required on 100 Gb or 25 Gb long-range optics because these optics do error correction internally.

For more information, see Administering VOSS.

Internet Protocol Flow Information eXport (IPFIX)

Internet Protocol Flow Information eXport (IPFIX) is an Internet Engineering Task Force (IETF) standard to export IP flow information. IPFIX monitors IPv4 traffic flows and exports flow information, such as source and destination IP address or the number of packets belonging to a specific flow, to a collector. The collector performs network analytics to provide statistical data.

This feature is specific to VSP 7400 Series.

For more information, see Monitoring Performance for VOSS.

IPv6 IS-IS Accept Policies

This release introduces support for IPv6 IS-IS accept policies. The IS-IS accept policies for IPv4 and IPv6 are independent, and can be configured separately.

For more information, see Configuring Fabric Layer 3 Services for VOSS.

IPv6 Virtualization

IPv6 Virtualization adds the ability to support the following IPv6 features in Virtual Routing and Forwarding (VRF) and Layer 3 Virtual Services Networks (L3 VSNs):

- Open Shortest Path First for IPv6 (OSPFv3)
- IPv6 Border Gateway Protocol (IPv6 BGP)
- IPv6 route redistribution enhancements

For more information, see Configuring IPv6 Routing for VOSS.

Licensing

As a result of the increase in BGP peer scaling to 256 on some VOSS platforms, licensing requirements are updated to reflect that you require a Premier or Premier with MACsec license to configure more than 16 BGP Peers.

Licensing is also updated to reflect the removal of the Premier or Premier with MACsec license requirement for DvR Leaf.

For more information about licensing, see Administering VOSS.

Multicast scaling enhancements

An Egress BEB currently creates a IP multicast tunnel termination record for each BEB in the network, with the anticipation that it may have received IP multicast traffic over SPB from each of those BEBs. This release introduces a design optimization where the Egress BEB creates the IP multicast tunnel termination records for only those Ingress BEBs from which it currently receives streams. As long as a given BEB is not expected to receive IP multicast traffic from all other BEBs in the network simultaneously, this change supports larger SPB networks. With this change, the VOSS products support being in SPB networks of up to 1,000 nodes. At this scale, the VSP 4000 Series can receive IP multicast over SPB traffic from up to 100 BEBs simultaneously and other VOSS products have no limitation on how many BEBs they can simultaneously receive traffic from.

For information on scaling, see Fabric Scaling on page 56.

NTPv4 enhancements

Starting with this release the switch can operate as both NTPv4 client and NTPv4 Server. You can configure the NTPv4 Server to operate in master mode. This release also introduces the NTPv4 Restrict capability on the switch that permits NTP traffic (with default restrictions) for all IP addresses or permits NTP traffic from the specified IP addresses or networks.

For more information, see Administering VOSS.

Representational State Transfer Configuration Protocol (RESTCONF)

Representational State Transfer Configuration Protocol (RESTCONF) is a next generation northbound interface that provides an additional way to configure and monitor the switch. RESTCONF is an HTTP-based protocol that provides a programmatic interface to access data defined in a YANG model using the datastore concepts defined in NETCONF. RESTCONF uses a client-server model. The server acts as an entry point to a datastore, a conceptual place to store and access information. Clients use HTTP or HTTPS to interface with the server to configure and monitor devices.

For more information, see Configuring User Interfaces and Operating Systems for VOSS.

TCP timestamp control

TCP Timestamp (RFC 1323) provides protection against Wrapped Seqence numbers. However, it is possible to calculate the system uptime when the Timestamp option is enabled. The analysis of timestamp behaviour can provide information on the system identity, which poses security threats and can cause a potential attack. This release introduces the option to enable or disable the TCP Timestamp.

For more information, see Configuring Security for VOSS.

Timestamp in show command outputs

The output for all CLI show commands includes a timestamp header to indicate when the command output was generated. This information can be helpful when communicating with Support.

For an example, see Configuring User Interfaces and Operating Systems for VOSS.

Two Factor Authentication for SSH

VOSS now supports Two Factor Authentication with smart cards, to authenticate users for SSH access to switches for device management. Two Factor Authentication leverages a Public Key Infrastucture (PKI) security certificate to verify a cardholder's identity prior to allowing access to protected resoures. You must enable Secure Shell (SSH) and X.509 V3 authorization on the switch,

and provide the digital certificates to enable the identity management for the SSH client and server. Two Factor Authentication requires: a VOSS switch as the SSH server, a PC with Secure CRT 8.3.2 or 8.3.3 as the SSH client, a smart card reader, and Common Access Card (CAC) or Personal Identity Verification (PIV) cards. Optionally you can use a Windows Server 2008 or newer configured with RADIUS server and Active Directory. The switches use SSH and X.509 V3 certificates stored on the smart card. X.509 V3 digital certificates are documented in RFC5280.

For more information, see Configuring Security for VOSS.

Filenames for this Release

Important:

Do not use Google Chrome or Safari to download software files. Google Chrome can change the file sizes. Safari changes the .tgz extension to .tar.

After you download the software, calculate and verify the md5 checksum. For more information, see Administering VOSS.

In VOSS 4.2 and later, the encryption modules are included as part of the standard runtime software image file.

Prior to VOSS 4.2.1, image filenames began with VSP, for example, `VSP4K4.1.0.0.tgz`. In VOSS 4.2.1 and later, image filenames start with VOSS, for example, `VOSS8K4.2.1.0.tgz`.

The Open Source license text for the switch is included on the product. You can access it by entering the following command in the CLI:

```
more release/w.x.y.z.GA /release/oss-notice.txt
```

where *w.x.y.z* represents a specific release number.

The following tables provide the filenames and sizes for this release.

Table 3: VSP 4450 Series Software Filenames and Sizes

Description	File	Size
SHA512 Checksum files	VOSS4K.8.0.0.0.sha512	1,388 bytes
MD5 Checksum files	VOSS4K.8.0.0.0.md5	524 bytes
MIB - supported object names	VOSS4K.8.0.0.0_mib_sup.txt	1,324,487 bytes
MIB - zip file of all MIBs	VOSS4K.8.0.0.0_mib.zip	1,141,661 bytes
MIB - objects in the OID compile order	VOSS4K.8.0.0.0_mib.txt	7,572,745 bytes
EDM Help files	VSP4000v800_HELP_EDM_gzip.zip	4,088,502 bytes
Logs reference	VOSS4K.8.0.0.0_edoc.tar	65,413,120 bytes

Table continues…

Description	File	Size
Software image	VOSS4K.8.0.0.0.tgz	123,442,513 bytes
Open source software - Master copyright file	VOSS4K.8.0.0.0_oss-notice.html	2,766,227 bytes
YANG model	restconf_yang.tgz	506,020

Table 4: VSP 7200 Series Software Filenames and Sizes

Description	File	Size
SHA512 Checksum files	VOSS7K.8.0.0.0.sha512	1,385 bytes
MD5 Checksum files	VOSS7K.8.0.0.0.md5	521 bytes
MIB - supported object names	VOSS7K.8.0.0.0_mib_sup.txt	1,327,309 bytes
MIB - zip file of all MIBs	VOSS7K.8.0.0.0_mib.zip	1,141,661 bytes
MIB - objects in the OID compile order	VOSS7K.8.0.0.0_mib.txt	7,572,745 bytes
EDM Help files	VOSSv800_HELP_EDM_gzip.zip	4,088,502 bytes
Logs reference	VOSS7K.8.0.0.0_edoc.tar	65,413,120 bytes
Software image	VOSS7K.8.0.0.0.tgz	137,547,781 bytes
Open source software - Master copyright file	VOSS7K.8.0.0.0_oss-notice.html	2,766,227 bytes
YANG model	restconf_yang.tgz	506,020

Table 5: VSP 7400 Series Software Filenames and Sizes

Description	File	Size
SHA512 Checksum files	VOSS7400.8.0.0.0.sha512	1,404
MD5 Checksum files	VOSS7400.8.0.0.0.md5	540
MIB - supported object names	VOSS7400.8.0.0.0_mib_sup.txt	1,335,435
MIB - zip file of all MIBs	VOSS7400.8.0.0.0_mib.zip	1,141,661
MIB - objects in the OID compile order	VOSS7400.8.0.0.0_mib.txt	7,572,745
EDM Help files	VSP7400v800_HELP_EDM_gzip.zip	4,088,502 bytes
Logs reference	VOSS7400.8.0.0.0_edoc.tar	65,413,120 bytes
Software image	VOSS7400.8.0.0.0.tgz	266,237,958
Open source software - Master copyright file	VOSS7400.8.0.0.0_oss-notice.html	2,766,227 bytes
YANG model	restconf_yang.tgz	506,020
Third Party Virtual Machine (TPVM)	TPVM_7400_8.0.0.0.img	1,724,252,160
Purview Engine Virtual Appliance	purview_7400_8.0.0.0.ova	1,762,308,608

Table 6: VSP 8000 Series Software Filenames and Sizes

Description	File	Size
SHA512 Checksum files	VOSS8K.8.0.0.0.sha512	1,385 bytes
MD5 Checksum files	VOSS8K.8.0.0.0.md5	521 bytes
MIB - supported object names	VOSS8K.8.0.0.0_mib_sup.txt	1,327,309 bytes
MIB - zip file of all MIBs	VOSS8K.8.0.0.0_mib.zip	1,141,661 bytes
MIB - objects in the OID compile order	VOSS8K.8.0.0.0_mib.txt	7,572,745 bytes
EDM Help files	VOSSv800_HELP_EDM_gzip.zip	4,088,502 bytes
Logs reference	VOSS8K.8.0.0.0_edoc.tar	65,413,120 bytes
Software image	VOSS8K.8.0.0.0.tgz	218,989,797 bytes
Open source software - Master copyright file	VOSS8K.8.0.0.0_oss-notice.html	2,766,227 bytes
YANG model	restconf_yang.tgz	506,020

Chapter 3: Upgrade and Downgrade Considerations

See the Administering VOSS document for detailed image management procedures that includes information about the following specific upgrade considerations:

- Notes for systems using IPv6 static neighbors
- Pre-upgrade instructions for IS-IS metric type
- Upgrade considerations regarding MACsec replay-protect configuration
- Upgrade support for the nni-mstp boot configuration flag
- Upgrade considerations for IS-IS enabled links with HMAC-MD5 authentication
- Considerations for IPv6 VRRP or DHCP Relay configurations saved in VOSS 4.1 or 4.2
- TACACS+ upgrade consideration

If your configuration includes one of the preceding scenarios, read the upgrade information in Administering VOSS before you begin an image upgrade.

Important:

Notice for VSP 4450GSX-PWR+, VSP 4450GSX, VSP 4450GTX-HT-PWR+, VSP 7200 Series, and VSP 8000 Series.

For these switch models running VOSS versions earlier than VOSS 6.1.x, you must first upgrade to VOSS 6.1.x before you can upgrade to VOSS 7.0 and later. Ensure that you save and back up your existing configuration before and after you upgrade to the intermediate 6.1.x release.

The same restriction applies to downgrades from VOSS 7.0 and later to releases earlier than VOSS 6.1.x. You must first downgrade to VOSS 6.1.x.

Supported Upgrade Paths

This section identifies the software releases for which upgrades to this release have been validated.

Supported Upgrade Paths for VSP 4450GSX-PWR+, VSP 4450GSX, VSP 4450GTX-HT-PWR+, VSP 7200 Series, and VSP 8000 Series

Validated upgrade paths are VOSS 6.1.x or VOSS 7.x to VOSS 8.0.

Release 7.0 introduced a new Linux kernel on these switch models. Upgrades to this release are only supported from VOSS 6.1.x and after.

For these switch models running older VOSS versions, you must first upgrade to 6.1.x before you can upgrade to VOSS 8.0. Ensure that you save and back up your existing configuration before and after you upgrade to the intermediate 6.1.x release.

Important:

If you upgrade to VOSS 8.0 and then need to downgrade to a release earlier than VOSS 6.1.x, you must also do so in steps by first downgrading to a VOSS 6.1.x release before downgrading to the desired release.

Upgrading DvR Configurations from Releases 6.0.1.1 and Earlier to 6.0.1.2 and Later

Upgrade all DvR nodes to the same release as quickly as possible. Release 6.0.1.2 includes changes to I-SID ranges that are utilized for DvR communication, and thus introduces an incompatibility with DvR nodes running 6.0.1.1 and earlier, with 6.0.1.2 and beyond.

Important:

Because of the change in 6.0.1.2, Extreme Networks recommends a *minimum* software version of 6.0.1.2 in DvR deployments.

Upgrade all DvR Leaf nodes first to minimize the impact of this incompatibility and the resulting loss of connectivity between DvR Controller nodes and Leaf nodes while nodes are at incompatible versions. After you upgrade all Leaf nodes, upgrade the Controller nodes, which restores DvR connectivity to the already upgraded Leaf nodes.

Important:

During the period of time when the Leaf nodes and Controller nodes are running incompatible versions, no DvR connectivity exists between the Controller and Leaf nodes so plan this activity accordingly, such as during a maintenance window.

If you cannot perform the upgrade during a maintenance window, use the following upgrade order to minimize connectivity loss:

1. Upgrade one of the DvR Controller nodes (vIST cluster member).
2. Upgrade the first DvR Leaf vIST cluster member.
3. Upgrade the second DvR Leaf vIST cluster member.
4. Upgrade the other DvR Controller.

By following the preceding list, you upgrade the first Controller and make it ready for the Leaf nodes as you upgrade them. The other Controller still uses the original software version to accommodate Leaf nodes yet to upgrade, which allows you to upgrade them one at a time. Upgrade the other Controller last. With this upgrade order, only the node you are upgrading experiences a connectivity loss.

Upgrading DvR Configuration from 6.0.1.0 or 6.0.1.1 to 6.1.x.x

To upgrade DvR Leaf nodes:

1. Use the **`no dvr leaf virtual-ist`** command on the Leaf nodes if vIST is configured.
2. Use the **`no dvr leaf`** command on the Leaf nodes.

   Important:

   Do not save the configuration.
3. Upgrade the software to 6.1.x.x on the Leaf nodes, and then reboot the nodes.

To upgrade DvR Controllers:

1. Use the **`no dvr controller`** command on the Controllers.

   Important:

   Do not save the configuration.
2. Upgrade the software to 6.1.x.x on the Controllers, and then reboot the Controllers.

Real Time Clock

The latest VSP switches have an updated real time clock (RTC) component, which is not compatible with some older software releases. If you have the new hardware, the switch prevents you from downgrading to an unsupported release.

The hardware revision number of the affected products has been updated to reflect this change. For each product in the affected product families, the following table identifies the hardware revisions, and higher, that contain the updated RTC component.

Model	Minimum Hardware Revision
VSP 4450GSX	11
VSP 4450GTX-HT-PWR+	11
VSP 7254XSQ and VSP 7254XTQ	13
VSP 8284XSQ	12
VSP 8404	10
VSP 8404C	12

The minimum versions of software required for proper functioning of the product with the new RTC component are as follows:

- 6.x software baseline – 6.1.6.0
- 7.x or later software baseline – 7.1.0.1

All other earlier software versions do not support the new RTC component.

Syslog RFC 5424 and Extreme Management Center Integration

For existing customers with saved configurations prior to VOSS 6.1.2.0 who are parsing the non RFC 5424 syslog format, the device defaults to the old format. When Extreme Management Center registers for syslog, it configures it to the RFC 5424 format and automatically changes the syslog and log formats.

Post Upgrade Configuration for Zero Touch Fabric configuration or Dynamic Nickname Assignment

If you want to use either, or both, of these features in VOSS 7.0 or later, the following sections identify the possible configuration combinations:

- Option 1: Enable Zero Touch Fabric Connect configuration and Dynamic Nickname on page 21
- Option 2: Enable Dynamic Nickname Assignment on page 22
- Option 3: Enable Zero Touch Fabric Connect configuration on page 22
- Option 4: Disable Zero Touch Fabric Connect configuration and Dynamic Nickname Assignment on page 23

For general steps about how to upgrade the switch software, see Administering VOSS.

Option 1: Enable Zero Touch Fabric configuration and Dynamic Nickname Assignment

1. Start the nodes with the VOSS 7.0 or later image in factory-default fabric mode.
   - Factory default fabric mode enables Zero Touch Fabric configuration.
   - The switch configures SPBM and IS-IS to the following default values:
     - SPBM instance 1
     - Primary BVID 4051 and secondary BVID 4052
     - System ID uses default value (derived from the chassis base MAC)
     - Manual area and nickname are zero
   - The switch creates and enables IS-IS interfaces on FAN ports.
2. IS-IS adjacencies are not formed.
3. IS-IS interfaces are in listening mode. These interfaces do not send HELLO PDUs because there is no IS-IS manual area configured. These interfaces listen for incoming HELLO PDUs
4. The node learns the IS-IS manual area from the first HELLO PDU it receives on any IS-IS interface. This learned area is called the Dynamically Learned Area (DLA).
5. The node uses the DLA to send HELLO PDUs on all active IS-IS interfaces and form adjacencies if the IS-IS parameters match.

6. If all nodes in the network started in Zero Touch Fabric configuration mode, configure the manual area on at least one to them, which has physical connectivity with the rest of the nodes using the FAN interfaces. This node is referred to as the *seed* node. The term seed node describes the starting event to build the SPB network if all nodes start in Zero Touch Fabric configuration mode.
7. If you insert the new node in a network where SPB is already configured and is connected using the FAN port to the node on its IS-IS interface, the adjacency with that node comes up if it uses the same default BVLANs mentioned above.
8. Because Dynamic Nickname Assignment is not configured yet, nodes become nickname clients. The clients become FAN members and start advertising FAN membership using TLV 147.
9. The FAN is established based on FAN endpoint membership.
10. Select a node and enable the nickname server.
11. After detecting a nickname server exists in the network, the nickname client sends a request for a nickname to the server.
12. The server assigns a nickname, which the client node learns.

Option 2: Enable Dynamic Nickname Assignment

1. Start the nodes with the VOSS 7.0 or later image with the existing configuration.
   - Zero Touch Fabric configuration is not enabled.
   - The SPBM and IS-IS configuration is based on the configuration file.
   - A manual area is configured.
2. Disable IS-IS.
3. Remove static nicknames on all nodes.
4. Nodes become nickname clients. The clients become FAN members and start advertising FAN membership using TLV 147.
5. The FAN is established based on FAN endpoint membership.
6. Select a node and enable the nickname server.
7. After detecting a nickname server exists in the network, the nickname client sends a request for a nickname to the server.
8. The server assigns a nickname, which the client node learns.

Option 3: Enable Zero Touch Fabric configuration

1. Start the nodes with the VOSS 7.0 or later image in factory-default fabric mode.
   - Factory default fabric mode enables Zero Touch Fabric configuration.
   - The switch configures SPBM and IS-IS to the following default values:
     - SPBM instance 1
     - Primary BVID 4051 and secondary BVID 4052
     - System ID uses default value (derived from the chassis base MAC)
     - Manual area and nickname are zero

- The switch creates and enables IS-IS interfaces on FAN ports.

2. IS-IS adjacencies are not formed.
3. IS-IS interfaces are in listening mode. These interfaces do not send HELLO PDUs because there is no IS-IS manual area configured. These interfaces listen for incoming HELLO PDUs
4. The node learns the IS-IS manual area from the first HELLO PDU it receives on any IS-IS interface. This learned area is called the Dynamically Learned Area (DLA).
5. The node uses the DLA to send HELLO PDUs on all active IS-IS interfaces and form adjacencies if the IS-IS parameters match.
6. If all nodes in the network started in Zero Touch Fabric configuration mode, configure the manual area on at least one to them, which has physical connectivity with the rest of the nodes using the FAN interfaces. This node is referred to as the *seed* node. The term seed node describes the starting event to build the SPB network if all nodes start in Zero Touch Fabric configuration mode.
7. If you insert the new node in a network where SPB is already configured and is connected using the FAN port to the node on its IS-IS interface, the adjacency with that node comes up if it uses the same default BVLANs mentioned above.
8. Configure static nicknames on all nodes.

Option 4: Disable Zero Touch Fabric configuration and Dynamic Nickname Assignment

1. Start the nodes with the VOSS 7.0 or later image with the existing configuration.
   - Zero Touch Fabric configuration is not enabled.
   - The SPBM and IS-IS configuration is based on the configuration file.
   - A manual area is configured.
   - Static nicknames are configured.
2. Dynamic Nickname Assignment server and clients do not start.

Chapter 4: Hardware and Software Compatibility

This section lists the hardware compatibility for all VOSS platforms.

VSP 4000 Series Hardware

Part number	Model number	Initial release	Supported new feature release			
			6.1.2	7.0	7.1	8.0
EC4400004-E6	VSP 4450GSX-DC	4.0.50	Y	Y	Y	Y
EC4400A03-E6	VSP 4450GTX-HT-PWR+	4.0.40	Y	Y	Y	Y
EC4400A05-E6	VSP 4450GSX-PWR+	4.0	Y	Y	Y	Y
EC4400A05-E6GS	VSP 4450GSX-PWR+ TAA Compliant	4.0.50	Y	Y	Y	Y
EC4800078-E6	VSP 4850GTS-DC	3.0	Y	Y	Y	N
EC4800A78-E6 EC4800A78-E6GS	VSP 4850GTS	3.0	Y	Y	Y	N
EC4800A88-E6 EC4800A88-E6GS	VSP 4850GTS-PWR+	3.0	Y	Y	Y	N

VSP 4000 Series Operational Note

Warning:

The USB FLASH drive on all models of VSP 4850 Series (factory built and converted from ERS 4850) is a permanent non-removable part of the switch that you must NEVER remove from the switch to ensure proper operation. Additionally, you must install the USB cover to ensure additional protection against removal. The USB FLASH drive on the VSP 4850 Series switch is uniquely and permanently bound to the operating system of the switch it is first used on and cannot be transferred to a different switch. Removal (and reinsertion) of the USB FLASH drive from the switch is not supported as it can permanently compromise the switch functionality and render it non-functional.

VSP 7200 Series Hardware

Part number	Model number	Initial release	Supported new feature release			
			6.1.2	7.0	7.1	8.0
EC720001F-E6	VSP 7254XSQ DC (front to back airflow)	4.2.1	Y	Y	Y	Y
EC7200A1B-E6 EC7200A1F-E6 B represents back to front airflow. F represents front to back airflow.	VSP 7254XSQ	4.2.1	Y	Y	Y	Y
EC720002F-E6	VSP 7254XTQ DC (Front to back airflow)	4.2.1	Y	Y	Y	Y
EC7200A2B-E6 EC7200A2F-E6 B represents back to front airflow. F represents front to back airflow.	VSP 7254XTQ	4.2.1	Y	Y	Y	Y
EC7200A3B-E6 EC7200A3F-E6 B represents back to front airflow. F represents front to back airflow.	VSP 7254XSQ Port Licensed	5.1	Y	Y	Y	Y
EC7200A4B-E6 EC7200A4F-E6 B represents back to front airflow. F represents front to back airflow.	VSP 7254XTQ Port Licensed	5.1	Y	Y	Y	Y

VSP 7200 Series Operational Notes

- The VSP 7254XSQ has a PHYless design, which is typical for Data Center top of rack switches. The benefits of a PHYless design are lower power consumption and lower latency. However, due to the PHYless design, the following transceivers are not supported:
  - AA1403017-E6: 1-port 10GBASE-LRM SFP+
  - AA1403016-E6: 1-port 10GBase-ZR/ZW SFP+

    The AA1403165 10GBASE-ZR CWDM DDI SFP+ transceiver can be substituted for AA1403016-E6 10GBASE-ZR/ZW SFP+

- Software partitions the switch into two logical slots: Slot 1 and Slot 2.
  - Slot 1: 10 Gbps ports: 1 - 48
  - Slot 2: 40 Gbps ports: 1 - 6
- Channelization is supported on the 40 Gbps QSFP+ ports.
- MACsec support:
  - MACsec is only supported on the VSP 7254XTQ 10 Gbps ports.
  - MACsec is not supported on VSP 7254XSQ 10 Gbps ports
  - MACsec is not supported on VSP 7254XTQ and VSP 7254XSQ 40 Gbps ports whether channelization is enabled or not.
- Port licensing support on the port licensed VSP 7254XSQ fiber switch:
  - 24 ports (Slot 1, ports 25 to 48) out of the 48 1/10 GbE SFP/SFP+ ports require a Port License to be unlocked.
  - two ports (Slot 2, ports 5 and 6) out of the six 40 GbE QSFP+ ports require a Port License to be unlocked.
- Port licensing support on the port licensed VSP 7254XTQ copper switch:
  - 24 ports (Slot 1, ports 25 to 48) out of the 48 100 Mbps/1 GbE/10 GbE RJ-45 ports require a Port License to be unlocked.
  - two ports (Slot 2, ports 5 and 6) out of the six 40 GbE QSFP+ ports require a Port License to be unlocked.
- 1000BASE-T SFP (AA1419043-E6) will only operate at 1 Gbps speeds when used on a VSP 7254XSQ.
- When you use 1 Gigabit Ethernet SFP transceivers on VSP 7254XSQ, the software disables auto-negotiation on the port:
  - If you use 1 Gbps fiber SFP transceivers, the remote end must also have auto-negotiation disabled.
  - If you use 1 Gbps copper SFP transceivers, the remote end must have auto-negotiation enabled. If not, the link will not be established.
- When a port on VSP 7254XSQ is disabled or enabled, or a cable replaced, or the switch rebooted, the remote link can flap twice.
- Enable auto-negotiation to ensure proper operation at 100 Mbps speeds on VSP 7254XTQ:
  - Link instability will be seen if both ends are set to 100 Mbps auto-negotiation disabled and you use a straight through cable.
  - If Link instability is seen when you use a cross-over cable, a port disable or enable can fix the issue.

VSP 7400 Series Hardware

Part number	Model Number	Initial release	Supported new feature release
			8.0
VSP7400-32C (no power supplies or fans) VSP7400-32C-AC-F (front-to-back airflow) VSP7400-32C-AC-R (back-to-front airflow)	VSP 7432CQ	8.0	Y

VSP 7400 Series Operational Notes

The VSP 7400 Series has a PHYless design. The benefits of a PHYless design are lower power consumption and lower latency. However, due to the PHYless design, the following transceivers are not supported:

- AA1403017-E6: 1-port 10GBASE-LRM SFP+
- AA1403016-E6: 1-port 10GBase-ZR/ZW SFP+

  The AA1403165 10GBASE-ZR CWDM DDI SFP+ transceiver can be substituted for AA1403016-E6 10GBASE-ZR/ZW SFP+

The following list provides operational notes for VSP 7432CQ.

- Ports 31 and 32 are reserved for internal use when Fabric Connect is used.
- The QSFP28 ports support the use of QSFP28 and QSFP+ transceivers:
  - The software detects the transceiver type and sets the port speed as either 100 Gbps for QSFP28 or 40 Gbps for QSFP+.
- Channelization:
  - Channelization is not supported on port 28.
  - Supports 4x10 Gbps when channelization is enabled and QSFP+ transceiver is detected.
  - Supports 4x25 Gbps when channelization is enabled and QSFP28 transceiver is detected.

VSP 8000 Series Hardware

Part number	Model number	Initial release	Supported new feature release			
			6.1.2	7.0	7.1	8.0
EC8200A01-E6 EC8200A01-E6GS	VSP 8284XSQ	4.0	Y	Y	Y	Y

Table continues…

Part number	Model number	Initial release	Supported new feature release			
			6.1.2	7.0	7.1	8.0
EC8200001-E6	VSP 8284XSQ DC	4.0.50	Y	Y	Y	Y
EC8400001-E6	VSP 8404 DC	4.2.1	Y	Y	Y	Y
EC8400A01-E6 EC8200A01-E6GS	VSP 8404	4.2	Y	Y	Y	Y
EC8400002-E6	VSP 8404C DC	5.3	Y	Y	Y	Y
EC8400A02-E6 EC8200A02-E6GS	VSP 8404C	5.3	Y	Y	Y	Y
Ethernet Switch Modules (ESM) — VSP 8400 Series only **Important:** Ensure the switch runs, at a minimum, the noted initial software release before you install an ESM.						
EC8404001-E6 EC8404001-E6GS	8424XS	4.2	Y	Y	Y	Y
EC8404002-E6 EC8404002-E6GS	8424XT	4.2	Y	Y	Y	Y
EC8404003-E6 EC8404003-E6GS	8408QQ	4.2	Y	Y	Y	Y
EC8404005-E6 EC8404005-E6GS	8418XSQ	4.2	Y	Y	Y	Y
EC8404006-E6 EC8404006-E6GS	8418XTQ	5.0	Y	Y	Y	Y
EC8404007-E6 EC8404007-E6GS	8424GS	5.0	Y	Y	Y	Y
EC8404008-E6 EC8404008-E6GS	8424GT	5.0	Y	Y	Y	Y
EC8404009-E6 EC8404009-E6GS	8402CQ Supported in VSP 8404C only	5.3	Y	Y	Y	Y

Transceivers

The software allows the use of transceivers and direct attach cables from any vendor, which means that the switch will bring up the port operationally when using any transceiver. Extreme Networks

does not provide support for operational issues related to the use of non-Extreme Networks branded transceivers and direct attached cables used in the switches.

Extreme Networks supports SFP transceivers with the following part numbers: AA1419013–E5, AA1419014–E5, AA1419015–E5, and AA1419025–E5 to AA1419040–E5. However, Extreme Networks strongly recommends using the newer DDI versions of these SFP transceivers.

Note:

Although VSP 8000 Series and VSP 7200 Series support 10 Gigabit and 40 Gigabit DAC cables in forgiving mode, in releases earlier than VOSS 4.2.1, the command output for **`show pluggable-optical-modules basic`** displays the corresponding vendor name rather than leaving the vendor name field blank.

The following table indicates where to find more information about optical transceivers and components.

Extreme Networks optical transceivers and components	*Extreme Networks Pluggable Transceivers Installation Guide*
Compatibility for Extreme Networks SFP, SFP+, QSFP+, and QSFP28 transceiver modules with the VSP series switches	VSP Components: SFP, SFP+, QSFP+, QSFP28 Support

Autonegotiation

Use Autonegotiation to allow the device to automatically negotiate the best common data rate and duplex mode to use between two Autonegotiation-capable Ethernet devices.

When you use a 1 Gigabit SFP transceiver on a 10 Gigabit SFP+ port, you must enable autonegotiate if it is not enabled already. However, if you use 1 Gigabit SFP transceivers on a VSP 4000 Series switch that is connected to third party switches at the remote end, you must have auto-negotiate enabled at all times; this applies to SFP transceivers installed in a 1 Gigabit SFP port or a 10 Gigabit SFP+ port.

For VSP 7254XSQ, auto-negotiation is always disabled for 1 Gigabit Ethernet transceivers. If using a 1000BASE-T SFP, the remote 1000BASE-T interface must have auto-negotiation enabled. If not, the link will not be established. Also note that because the SFP+ ports on the VSP 7254XSQ only support 1 and 10 Gbps speeds, the AA1419043-E6 1000BASE-T SFP will only operate at 1G speeds.

If you use 1 Gbps fiber SFP transceivers, auto-negotiation is always disabled so the remote end must also have auto-negotiation disabled. Otherwise this is not a supported configuration with VSP 7254XSQ.

Forward Error Correction (FEC)

Forward Error Correction (FEC) is a method of obtaining error control in data transmission over an unreliable or noisy channel in which the source (transmitter) encodes the data in a redundant way by using an error correcting code (ECC). This redundancy enables a destination (receiver) to detect a limited number of errors and correct them without requiring a re-transmission.

For more information about FEC, see Administering VOSS.

Power Supply Compatibility

You can use certain power supplies in more than one VOSS platform. This section lists the power supplies and indicates the compatible platforms.

For more specific information on each power supply, see the following documents:

- Installing the Virtual Services Platform 4850GTS Series
- Installing the Virtual Services Platform 4450GTX-HT-PWR+
- Installing the Virtual Services Platform 4450GSX-PWR+
- Installing the Virtual Services Platform 7200 Series
- VSP 7400 Series Switches: Hardware Installation Guide
- Installing the Virtual Services Platform 8000 Series

Table 7: VSP 4000 Series Power Supplies

Platform	300 W AC AL1905A08-E5	300 W DC AL1905005-E5	1,000 W AC AL1905A21-E6	1,000 W AC-HT EC4005A03-E6HT
VSP 4850GTS-DC	—	Y	—	—
VSP 4850GTS-PWR+	—	—	Y	Y
VSP 4850GTS	Y	—	—	—
VSP 4450GTX-HT-PWR+	—	—	—	Y
VSP 4450GSX-DC	—	Y	—	—
VSP 4450GSX-PWR+	—	—	Y	Y

Table 8: VSP 7200 Series and VSP 8000 Series Power Supplies

Platform	460 W AC front-to-back EC7205A1F-E6	460 W AC back-to-front EC7205A1B-E6	800 W AC front-to-back EC8005A01-E6	800 W AC front-to-back EC7205A0F-E6	800 W AC back-to-front EC7205A0B-E6	800 W DC front-to-back EC8005001-E6
VSP 8284XSQ	—	—	Y	—	—	—
VSP 8284XSQ DC	—	—	—	—	—	Y
VSP 8404	—	—	Y	—	—	—
VSP 8404 DC	—	—	—	—	—	Y
VSP 8404C	—	—	Y	—	—	—
VSP 8404C DC	—	—	—	—	—	Y

Table continues…

Platform	460 W AC front-to-back EC7205A1F-E6	460 W AC back-to-front EC7205A1B-E6	800 W AC front-to-back EC8005A01-E6	800 W AC front-to-back EC7205A0F-E6	800 W AC back-to-front EC7205A0B-E6	800 W DC front-to-back EC8005001-E6
VSP 7254XSQ front-to-back	Y	—	—	—	—	—
VSP 7254XSQ back-to-front	—	Y	—	—	—	—
VSP 7254XTQ front-to-back	—	—	—	Y	—	—
VSP 7254XTQ back-to-front	—	—	—	—	Y	—
VSP 7254XSQ DC	—	—	—	—	—	Y
VSP 7254XTQ DC	—	—	—	—	—	Y

Table 9: VSP 7400 Series Power Supplies

Platform	750 W AC front-to-back XN-ACPWR-750W-F	750 W AC back-to-front XN-ACPWR-750W-R	750 W DC front-to-back XN-DCPWR-750W-F	750 W DC back-to-front XN-DCPWR-750W-R
VSP 7432CQ front-to-back	Y	—	—	—
VSP 7432CQ back-to-front	—	Y	—	—
VSP 7432CQ front-to-back DC	—	—	Y	—
VSP 7432CQ back-to-front DC	—	—	—	Y

Chapter 5: Scaling

This section documents scaling capabilities of the VOSS platforms.

The scaling and performance information shown in the following tables is provided for the purpose of assisting with network design. It is recommended that network architects and administrators design and manage networks with an appropriate level of network scaling “head room.” The scaling and performance figures provided have been verified using specific network topologies using limited switch configurations. There is no guarantee that the scaling and performance figures shown are applicable to all network topologies and switch configurations and are provided as a realistic estimation only. If you experience scaling and performance characteristics that you feel are sufficiently below what has been documented, contact Extreme Networks technical support for additional assistance.

Note:

If your switch uses Advanced Feature Bandwidth Reservation in Full Feature mode, this affects scaling information that is based on the number of available ports. If you enable the boot configuration flag for this feature, remember to deduct the number of reserved ports from the documented scaling maximum. Not all hardware platforms require this feature to provide full feature support. For feature support information, see Features by Release on page 99.

Layer 2

Table 10: Layer 2 Maximums

Attribute	Product	Maximum number supported
Directed Broadcast interfaces **Note:** The number of Directed Broadcast interfaces must be less than or equal to 200. However, if you configure VLANs with both NLB and Directed Broadcast, you can only scale up to 100 VLANs.	VSP 4450 Series	n/a
	VSP 7200 Series	200 See Note.
	VSP 7400 Series	200 See Note.
	VSP 8000 Series	200 See Note.

Table continues…

Attribute	Product	Maximum number supported
MAC table size (without SPBM)	VSP 4450 Series	32,000
	VSP 7200 Series	224,000
	VSP 7400 Series	160,000
	VSP 8000 Series	224,000
MAC table size (with SPBM)	VSP 4450 Series	16,000
	VSP 7200 Series	112,000
	VSP 7400 Series	80,000
	VSP 8000 Series	112,000
Port-based VLANs	VSP 4450 Series	4,059
	VSP 7200 Series	4,059
	VSP 7400 Series	4,059
	VSP 8000 Series	4,059
Private VLANs	VSP 4450 Series	200
	VSP 7200 Series	200
	VSP 7400 Series	200
	VSP 8000 Series	VSP 8404C = 400 Other VSP 8000 Series platforms = 200
Protocol-based VLANs (IPv6 only)	VSP 4450 Series	1
	VSP 7200 Series	1
	VSP 7400 Series	1
	VSP 8000 Series	1
RSTP instances	VSP 4450 Series	1
	VSP 7200 Series	1
	VSP 7400 Series	1
	VSP 8000 Series	1
MSTP instances	VSP 4450 Series	12
	VSP 7200 Series	12
	VSP 7400 Series	64
	VSP 8000 Series	12
LACP aggregators	VSP 4450 Series	24
	VSP 7200 Series	54 (up to 72 with channelization)
	VSP 7400 Series	32 (up to 125 with channelization) with

Table continues…

Attribute	Product	Maximum number supported
		Advanced Feature Bandwidth Reservation configured in Full Port mode
	VSP 8000 Series	84 (up to 96 with channelization)
Ports per LACP aggregator	VSP 4450 Series	8 active
	VSP 7200 Series	8 active
	VSP 7400 Series	8 active
	VSP 8000 Series	8 active
MLT groups	VSP 4450 Series	50
	VSP 7200 Series	54 (up to 72 with channelization)
	VSP 7400 Series	32 (up to 125 with channelization) with Advanced Feature Bandwidth Reservation configured in Full Port mode
	VSP 8000 Series	84 (up to 96 with channelization)
Ports per MLT group	VSP 4450 Series	8
	VSP 7200 Series	8
	VSP 7400 Series	8
	VSP 8000 Series	8
LST groups	VSP 4450 Series	48
	VSP 7200 Series	48
	VSP 7400 Series	n/a
	VSP 8000 Series	48
Interfaces per LST group	VSP 4450 Series	8 upstream 128 downstream
	VSP 7200 Series	8 upstream 128 downstream
	VSP 7400 Series	n/a
	VSP 8000 Series	8 upstream 128 downstream
SLPP VLANs	VSP 4450 Series	128

Table continues…

Attribute	Product	Maximum number supported
	VSP 7200 Series	128
	VSP 7400 Series	500
	VSP 8000 Series	128
VLACP interfaces	VSP 4450 Series	50
	VSP 7200 Series	54 (up to 72 with channelization)
	VSP 7400 Series	32 (up to 125 with channelization) with Advanced Feature Bandwidth Reservation configured in Full Port mode
	VSP 8000 Series	84 (up to 96 with channelization)
Microsoft NLB cluster IP interfaces **Note:** The number of NLB cluster IP interfaces multiplied by the number of configured clusters must be less than or equal to 200. The number of NLB cluster IP interfaces is the key, not the number of VLANs. You can configure 1 VLAN with up to 200 NLB cluster IP interfaces or configure up to 200 VLANs with 1 NLB cluster IP interface per VLAN. For example: 1 virtual interface per cluster x 200 clusters = 200 or 2 virtual interfaces per cluster x 100 clusters = 200 However, if you configure VLANs with both NLB and Directed Broadcast, you can only scale up to 100 VLANs assuming there is only 1 NLB cluster IP interface per VLAN.	VSP 4450 Series	n/a
	VSP 7200 Series	200 See Note.
	VSP 7400 Series	200 See Note.
	VSP 8000 Series	200 See Note.

IP Unicast

Table 11: IP Unicast Maximums

Attribute	Product	Maximum number supported
Note: The maximum number of IP interfaces is based on the following formulas: • For VSP 7200 Series, VSP 8200 Series, and VSP 8400 Series: - If you disable the VRF scaling boot configuration flag: • = 506 – (# of VRRP IPv4 interfaces) - (# of VRRP IPv6 interfaces) – (# of RSMLT interfaces) – 2 (if IP Shortcuts is enabled) – 3x(# of VRFs) - If you enable the VRF scaling boot configuration flag: • = 506 – (# of VRRP IPv4 interfaces) – (# of VRRP IPv6 interfaces) - (# of RSMLT interfaces) – 2 (if IP Shortcuts is enabled) – 3 • For VSP 7400 Series: - If you disable the VRF scaling boot configuration flag: • = 1000 – (# of VRRP IPv4 interfaces) - (# of VRRP IPv6 interfaces) – (# of RSMLT interfaces) – 2 (if IP Shortcuts is enabled) – 3x(# of VRFs) - If you enable the VRF scaling boot configuration flag: • = 1000 – (# of VRRP IPv4 interfaces) – (# of VRRP IPv6 interfaces) - (# of RSMLT interfaces) – 2 (if IP Shortcuts is enabled) – 3		
IP interfaces (IPv4 or IPv6 or IPv4+IPv6)	VSP 4450 Series	256
	VSP 7200 Series	506 See Note.
	VSP 7400 Series	1,000 See Note.
	VSP 8000 Series	VSP 8404C = 503 Other VSP 8000 Series platforms = 506 See Note.
VRRP interfaces (IPv4 or IPv6)	VSP 4450 Series	64
	VSP 7200 Series	252 See Note.
	VSP 7400 Series	500 See Note.

Table continues…

Attribute	Product	Maximum number supported
	VSP 8000 Series	252 See Note.
Routed Split Multi-Link Trunking (RSMLT) interfaces (IPv4 or IPv6 or IPv4+IPv6)	VSP 4450 Series	252
	VSP 7200 Series	252 See Note.
	VSP 7400 Series	500 See Note.
	VSP 8000 Series	252 See Note.
VRRP interfaces with fast timers (200ms) - IPv4/IPv6	VSP 4450 Series	24
	VSP 7200 Series	24
	VSP 7400 Series	24
	VSP 8000 Series	24
DvR Virtual IP interfaces	VSP 4450 Series	501 with vIST 502 without vIST
	VSP 7200 Series	501 with vIST 502 without vIST
	VSP 7400 Series	501 with vIST 502 without vIST
	VSP 8000 Series	501 with vIST 502 without vIST
ECMP groups/paths per group	VSP 4450 Series	500/4
	VSP 7200 Series	1,000/8
	VSP 7400 Series	1,000/8
	VSP 8000 Series	1,000/8
OSPF v2/v3 interfaces	VSP 4450 Series	100
	VSP 7200 Series	500
	VSP 7400 Series	500
	VSP 8000 Series	500
OSPF v2/v3 neighbors (adjacencies)	VSP 4450 Series	100
	VSP 7200 Series	500
	VSP 7400 Series	500
	VSP 8000 Series	500
OSPF areas	VSP 4450 Series	12 for each VRF

Table continues…

Attribute	Product	Maximum number supported
		64 for the switch
	VSP 7200 Series	12 for each VRF 80 for the switch
	VSP 7400 Series	12 for each VRF 80 for the switch
	VSP 8000 Series	12 for each VRF 80 for the switch
IPv4 ARP table	VSP 4450 Series	6,000
	VSP 7200 Series	32,000
	VSP 7400 Series	56,000 non-SPB deployments 40,000 SPB deployments
	VSP 8000 Series	32,000
IPv4 CLIP interfaces	VSP 4450 Series	64
	VSP 7200 Series	64
	VSP 7400 Series	64
	VSP 8000 Series	64
IPv4 RIP interfaces	VSP 4450 Series	24
	VSP 7200 Series	200
	VSP 7400 Series	200
	VSP 8000 Series	200
IPv4 BGP peers	VSP 4450 Series	12
	VSP 7200 Series	256
	VSP 7400 Series	256
	VSP 8000 Series	256
IPv4 VRF instances For additional information, see VRF Scaling on page 62.	VSP 4450 Series	128 including GRT
	VSP 7200 Series	256 including mgmt VRF and GRT
	VSP 7400 Series	256 including mgmt VRF and GRT
	VSP 8000 Series	256 including mgmt VRF and GRT
IPv4 static ARP entries	VSP 4450 Series	200 for each VRF 1,000 for the switch
	VSP 7200 Series	2,000 for each VRF

Table continues…

Attribute	Product	Maximum number supported
		10,000 for the switch
	VSP 7400 Series	2,000 for each VRF 10,000 for the switch
	VSP 8000 Series	2,000 for each VRF 10,000 for the switch
IPv4 static routes	VSP 4450 Series	1,000 for each VRF 1,000 for the switch
	VSP 7200 Series	1,000 for each VRF 5,000 for the switch
	VSP 7400 Series	1,000 for each VRF 5,000 for the switch
	VSP 8000 Series	1,000 for each VRF 5,000 for the switch
IPv4 route policies	VSP 4450 Series	500 for each VRF 5,000 for the switch
	VSP 7200 Series	500 for each VRF 5,000 for the switch
	VSP 7400 Series	2,000 for each VRF 16,000 for the switch
	VSP 8000 Series	500 for each VRF 5,000 for the switch
IPv4 UDP forwarding entries	VSP 4450 Series	128
	VSP 7200 Series	512
	VSP 7400 Series	1,024
	VSP 8000 Series	512
IPv4 DHCP Relay forwarding entries	VSP 4450 Series	128
	VSP 7200 Series	1,024
	VSP 7400 Series	1,024
	VSP 8000 Series	1,024
IPv6 DHCP Snoop entries in Source Binding Table	VSP 4450 Series	1,024
	VSP 7200 Series	1,024
	VSP 7400 Series	1,024
	VSP 8000 Series	1,024
IPv6 Neighbor table	VSP 4450 Series	4,000

Table continues…

Attribute	Product	Maximum number supported
	VSP 7200 Series	8,000
	VSP 7400 Series	32,000
	VSP 8000 Series	8,000
IPv6 static entries in Source Binding Table	VSP 4450 Series	256
	VSP 7200 Series	256
	VSP 7400 Series	256
	VSP 8000 Series	256
IPv6 static neighbor records	VSP 4450 Series	128
	VSP 7200 Series	128 per VRF 512 per system
	VSP 7400 Series	128 per VRF 512 per system
	VSP 8000 Series	128 per VRF 512 per system
IPv6 CLIP interfaces	VSP 4450 Series	64
	VSP 7200 Series	64
	VSP 7400 Series	64
	VSP 8000 Series	64
IPv6 static routes	VSP 4450 Series	1,000
	VSP 7200 Series	1,000
	VSP 7400 Series	1,000
	VSP 8000 Series	1,000
IPv6 6in4 configured tunnels	VSP 4450 Series	64
	VSP 7200 Series	64
	VSP 7400 Series	64
	VSP 8000 Series	64
IPv6 DHCP Relay forwarding	VSP 4450 Series	128
	VSP 7400 Series	512
	VSP 7200 Series	512
	VSP 8000 Series	512
IPv6 BGP peers	VSP 4450 Series	12 Up to 8,000 IPv6 prefixes for BGPv6 peering
	VSP 7200 Series	256

Table continues…

Attribute	Product	Maximum number supported
		Up to 8,000 IPv6 prefixes for BGPv6 peering
	VSP 7400 Series	256
	VSP 8000 Series	256 Up to 8,000 IPv6 prefixes for BGPv6 peering

Layer 3 Route Table Size

Table 12: Layer 3 Route Table Size Maximums

Attribute	Maximum number supported
IPv4 RIP routes	See Route Scaling on page 41.
IPv4 OSPF routes	
IPv4 BGP routes	
IPv4 SPB shortcut routes	
IPv4 SPB Layer 3 VSN routes	
IPv6 OSPFv3 routes - GRT only	
IPv6 SPB shortcut routes - GRT only	
IPv6 RIPng routes	

Route Scaling

The following table provides information on IPv4 and IPv6 route scaling. The route table is a shared hardware resource where IPv4 routes consume one entry and IPv6 routes with a prefix length less than 64 consume two entries.

The route scaling does not depend on the protocol itself, but rather the general system limitation in the following configuration modes:

- URPF check mode - Enable this boot configuration flag to support Unicast Reverse Path Forwarding check mode.
- IPv6 mode - Enable this boot configuration flag to support IPv6 routes with prefix-lengths greater than 64 bits. When the IPv6-mode is enabled, the maximum number of IPv4 routing table entries decreases. This flag does not apply to all hardware platforms.

Table 13: VSP 4450 Series, VSP 7200 Series, and VSP 8000 Series

URPF mode	IPv6 mode	VSP 4450 Series			VSP 7200 Series and VSP 8000 Series		
		IPv4	IPv6		IPv4	IPv6	
			Prefix less than 64	Prefix greater than 64		Prefix less than 64	Prefix greater than 64
No	No	15,744	7,887	256	15,488	7,744	n/a
No	Yes	n/a	n/a	n/a	7,488	3,744	2,000
Yes	No	7,744	3,872	256	7,488	3,744	n/a
Yes	Yes	n/a	n/a	n/a	3,488	1,744	1,000

Note:

The stated numbers in the preceding rows are one-dimensional where the given number implies that *only* routes for that address family or type are present. For a given row in the table, the maximum scaling number is ‘x’ IPv4 routes *OR* ‘y’ ipv6 <= 64 routes *OR* ‘z’ ipv6 >64 routes (not a combination of all).

Table 14: VSP 7400 Series

URPF mode	IPv6 mode	VSP 7400 Series		
		IPv4	IPv6	
			Prefix less than 64	Prefix greater than 64
No	No	15,000	7,000	n/a
No	Yes	7,000	3,500	2,000
Yes	No	7,000	3,500	n/a
Yes	Yes	3,000	1,500	1,000

Note:

The stated numbers in the preceding rows are one-dimensional where the given number implies that *only* routes for that address family or type are present. For a given row in the table, the maximum scaling number is ‘x’ IPv4 routes *OR* ‘y’ ipv6 <= 64 routes *OR* ‘z’ ipv6 >64 routes (not a combination of all).

IP Multicast

Table 15: IP Multicast Maximums

Attribute	Product	Maximum number supported
Combination of VLANs + number of IPv4 senders + IPv6 senders (non-SPBM mode)	VSP 4450 Series	4,059
	VSP 7200 Series	8,192
	VSP 7400 Series	8,192
	VSP 8000 Series	8,192
Combination of Layer 2 VSNs + number of IPv4 senders + number of IPv6 senders (SPBM mode)	VSP 4450 Series	4,059
	VSP 7200 Series	8,192
	VSP 7400 Series	8,192
	VSP 8000 Series	8,192
IGMP/MLD interfaces (IPv4/IPv6)	VSP 4450 Series	4,059
	VSP 7200 Series	4,059
	VSP 7400 Series	4,059
	VSP 8000 Series	4,059
PIM interfaces (IPv4/IPv6)	VSP 4450 Series	128 Active
	VSP 7200 Series	128 Active
	VSP 7400 Series	128 Active
	VSP 8000 Series	128 Active
PIM Neighbors (IPv4/IPv6) (GRT Only)	VSP 4450 Series	128
	VSP 7200 Series	128
	VSP 7400 Series	128
	VSP 8000 Series	128
PIM-SSM static channels (IPv4/IPv6)	VSP 4450 Series	512
	VSP 7200 Series	4,000
	VSP 7400 Series	4,000
	VSP 8000 Series	4,000
Multicast receivers/IGMP joins (IPv4/IPv6) (per switch)	VSP 4450 Series	1,000
	VSP 7200 Series	6,000
	VSP 7400 Series	6,000
	VSP 8000 Series	6,000
Total multicast routes (S,G,V) (IPv4/IPv6) (per switch)	VSP 4450 Series	1,000
	VSP 7200 Series	6,000
	VSP 7400 Series	6,000

Table continues…

Attribute	Product	Maximum number supported
	VSP 8000 Series	6,000
Total multicast routes (S,G,V) (IPv4) on an SPB-PIM Gateway configured switch	VSP 4450 Series	1,000
	VSP 7200 Series	3,000
	VSP 7400 Series	3,000
	VSP 8000 Series	3,000
Static multicast routes (S,G,V) (IPv4/IPv6)	VSP 4450 Series	512
	VSP 7200 Series	4,000
	VSP 7400 Series	4,000
	VSP 8000 Series	4,000
Multicast enabled Layer 2 VSN (IPv4)	VSP 4450 Series	1,000
	VSP 7200 Series	2,000
	VSP 7400 Series	2,000
	VSP 8000 Series	2,000
Multicast enabled Layer 3 VSN (IPv4)	VSP 4450 Series	128 including mgmt VRF and GRT
	VSP 7200 Series	256 including mgmt VRF and GRT
	VSP 7400 Series	256 including mgmt VRF and GRT
	VSP 8000 Series	256 including mgmt VRF and GRT
SPB-PIM Gateway controller S,Gs (source announcements) with MSDP (IPv4)	VSP 4450 Series	6,000
	VSP 7200 Series	6,000
	VSP 7400 Series	6,000
	VSP 8000 Series	6,000
SPB-PIM Gateway controllers per SPB fabric (IPv4)	VSP 4450 Series	5
	VSP 7200 Series	5
	VSP 7400 Series	5
	VSP 8000 Series	5
SPB-PIM Gateway nodes per SPB fabric (IPv4)	VSP 4450 Series	64
	VSP 7200 Series	64
	VSP 7400 Series	64
	VSP 8000 Series	64
SPB-PIM Gateway interfaces per BEB (IPv4)	VSP 4450 Series	64
	VSP 7200 Series	64

Table continues…

Attribute	Product	Maximum number supported
	VSP 7400 Series	64
	VSP 8000 Series	64
PIM neighbors per SPB-PIM Gateway node (IPv4)	VSP 4450 Series	64
	VSP 7200 Series	64
	VSP 7400 Series	64
	VSP 8000 Series	64

Distributed Virtual Routing (DvR)

Table 16: DvR Maximums

Attribute	Product	Maximum number supported
Note: • On the DvR leaf, you must enable the VRF scaling boot configuration flag if more than 24 VRFs are required in the DvR domain. • Scaling of the VSP 4450 Series controls the scaling of the DvR domain it is in. For example, if a VSP 4450 Series switch is in a DvR domain with other platforms such as VSP 7200 Series and VSP 8000 Series, the scaling of the entire domain is limited to the scaling of the VSP 4450 Series.		
DvR Virtual IP interfaces	VSP 4450 Series	501 with vIST 502 without vIST
	VSP 7200 Series	501 with vIST 502 without vIST
	VSP 7400 Series	501 with vIST 502 without vIST
	VSP 8000 Series	501 with vIST 502 without vIST
DvR domains per SPB fabric	VSP 4450 Series	16
	VSP 7200 Series	16
	VSP 7400 Series	16
	VSP 8000 Series	16
Controller nodes per DvR domain with default route inject flag enabled	VSP 4450 Series	n/a
	VSP 7200 Series	8
	VSP 7400 Series	8

Table continues…

Attribute	Product	Maximum number supported
Total number of Controllers per domain cannot exceed 8. **Note:** A DvR domain containing only Controller nodes and no Leaf nodes can have more than 8 Controllers per domain.	VSP 8000 Series	8
Leaf nodes per DvR domain	VSP 4450 Series	250
	VSP 7200 Series	250
	VSP 7400 Series	250
	VSP 8000 Series	250
DvR enabled Layer 2 VSNs	VSP 4450 Series	501 with vIST 502 without vIST
	VSP 7200 Series	501 with vIST 502 without vIST
	VSP 7400 Series	501 with vIST 502 without vIST
	VSP 8000 Series	501 with vIST 502 without vIST
DvR host rout scaling per DvR domain (scaling number includes local as well as foreign hosts of the Layer 2 VSN that are members of the domain) Total host route scaling across all domains cannot exceed 32,000.	VSP 4450 Series	6,000
	VSP 7200 Series	32,000
	VSP 7400 Series	32, 000
	VSP 8000 Series	32,000

VXLAN Gateway

Table 17: VXLAN Gateway Maximums

Attribute	Product	Maximum number supported
MAC addresses in base interworking mode	VSP 4450 Series	n/a
	VSP 7200 Series	112,000
	VSP 7400 Series	80,000
	VSP 8000 Series	112,000

Table continues…

Attribute	Product	Maximum number supported
MAC addresses in full interworking mode	VSP 4450 Series	n/a
	VSP 7200 Series	74,000
	VSP 7400 Series	50,000
	VSP 8000 Series	74,000
VNI IDs per node	VSP 4450 Series	n/a
	VSP 7200 Series	2,000
	VSP 7400 Series	2,000
	VSP 8000 Series	VSP 8404C = 4,000 Other VSP 8000 Series platforms = 2,000
VTEP destinations per node or VTEP	VSP 4450 Series	n/a
	VSP 7200 Series	500
	VSP 7400 Series	500
	VSP 8000 Series	500

The following table provides maximum numbers for OVSDB protocol support for VXLAN Gateway.

Table 18: OVSDB protocol support for VXLAN Gateway Maximums

Attribute	Product	Maximum number supported
Maximum controllers to which a single VTEP switch can connect	VSP 4450 Series	n/a
	VSP 7200 Series	3
	VSP 7400 Series	3
	VSP 8000 Series	3

Filters, QoS, and Security

Table 19: Filters, QoS, and Security Maximums

Attribute	Product	Maximum number supported
For more information, see Filter Scaling on page 49.		
Total IPv4 Ingress rules/ACEs (Port/VLAN/InVSN based, Security/QoS filters)	VSP 4450 Series	1,020
	VSP 7200 Series	766
	VSP 7400 Series	1,536

Table continues…

Attribute	Product	Maximum number supported
	VSP 8000 Series	VSP 8404C = 3,070 Other VSP 8000 Series platforms = 766
Total IPv4 Egress rules/ACEs (Port based, Security filters)	VSP 4450 Series	255 200 if you enable the ipv6-egress-filter boot configuration flag
	VSP 7200 Series	252 200 if you enable the ipv6-egress-filter boot configuration flag
	VSP 7400 Series	783 271 if you enable the ipv6-egress-filter boot configuration flag
	VSP 8000 Series	VSP 8404 and VSP 8404C = 251 Other VSP 8000 Series platforms = 252 200 if you enable the ipv6-egress-filter boot configuration flag
Total IPv6 Ingress rules/ACEs (Port/VLAN/InVSN based, Security filters)	VSP 4450 Series	255
	VSP 7200 Series	256
	VSP 7400 Series	767
	VSP 8000 Series	VSP 8404 = 511 VSP 8404C = 2,047 Other VSP 8000 Series platforms = 256
Total IPv6 egress rules/ACEs (Port based, Security filters)	VSP 4450 Series	256
	VSP 7200 Series	256
	VSP 7400 Series	511
	VSP 8000 Series	256
EAP and NEAP (clients per port)	VSP 4450 Series	32 for EAP 8,192 for NEAP
	VSP 7200 Series	32 for EAP 8,192 for NEAP

Table continues…

Attribute	Product	Maximum number supported
Note: The total of EAP clients plus NEAP clients per port or per switch cannot exceed 8,192.	VSP 7400 Series	32 for EAP 8,192 for NEAP
	VSP 8000 Series	32 for EAP 8,192 for NEAP

Filter Scaling

This section provides more details on filter scaling numbers for the VOSS platforms.

VSP 4450 Series

The switch supports the following maximum limits:

- 220 IPv4 ingress ACLs
- 50 IPv4 egress ACLs
- 128 IPv6 ingress ACLs
- 1,020 IPv4 ingress ACEs
- 252 IPv4 egress ACEs
- 255 IPv6 ingress ACEs
- 255 IPv6 egress ACEs

VSP 7400 Series

The switch supports the following maximum limits for *ACL* scaling:

- 512 non-IPv6 ingress ACLs (inPort or inVlan):
  - 256 ACLs with 1 Security ACE each + 256 ACLs with 1 QoS ACE each OR
  - 384 ACLs with 1 Security ACE each and/or 1 QoS ACE each OR
  - a combination based on the following rule:
    - `num ACLs <= 512 && (num ACLs + num Security ACEs) <= 512 && (num ACLs + num QoS ACEs) <= (512 – X)` where X = num IPv6 ACLs + num IPv6 ACEs

  This maximum implies a single port on inPort ACLs, and a single VLAN on inVlan ACLs.
- 384 IPv6 ingress ACLs (inPort):
  - 384 IPv6 ACLs with 1 Security ACE each OR
  - A combination based on the following rule:
    - `num IPv6 ACLs <= 384 && (num IPv6 ACLs + num Security ACEs) <= (768 – X)` where X = num non-IPv6 ACLs + num non-IPv6 QoS ACEs

  This maximum implies a single port on inPort ACLs.

- 254 non-IPv6 egress ACLs (outPort):
  - 254 ACLS with 1 Security ACE each OR
    - A combination based on the following rule:
      - `num ACLs <= 254 && (num ACLs + num Security ACEs) <= 508`

  This maximum implies a single port on outPort ACLs.
- 256 IPv6 Egress ACLs (outPort):
  - 256 ACLS with 1 Security ACE each OR
  - A combination based on the following rule:
    - `num ACLs <= 256 && (num ACLs + num Security ACEs) <= 512`

  This maximum implies a single port on outPort ACLs.

The switch supports the following maximum limits for *ACE* scaling:

- 1,536 non-IPv6 ingress ACEs

  This theoretical maximum implies
  - 1 non-IPv6 ingress ACL with 768 Security ACEs and 768 QoS ACEs
  - no IPv6 ACLs configured
  - a single port on inPort ACLs, and a single VLAN on inVLAN ACLs
- 768 IPv6 ingress ACEs

  This theoretical maximum implies
  - 1 IPv6 ingress ACL with 768 Security ACEs
  - no non-IPv6 ACLs configured
  - a port member count of 1 for inPort ACLs
- 783 non-IPv6 egress ACEs.

  This theoretical maximum implies
  - 1 egress ACL with 783 Security ACEs
  - a port member count of 1 for outPort ACLs
  - Non IPv6 egress ACEs supported: `784 - num non-IPv6 egress ACLs`
- 511 IPv6 egress ACEs

  This theoretical maximum implies
  - 1 egress ACL with 511 Security ACEs
  - a port member count of 1 for ourPort ACLs
  - `511 - num IPv6 egress ACLs`

VSP 7200 Series , VSP 8200 Series, and VSP 8404

The switch supports the following maximum limits:

- 256 ingress ACLs (inPort, inVSN, or inVlan):
  - 256 ACLs with 1 security ACE each OR
  - 128 ACLs with 1 QoS ACE each OR
  - a combination based on the following rule:
    - `( (num ACLs + num security ACEs) <= 512) && ((num ACLs + num QoS ACEs) <= 256)`

  This maximum implies a VLAN member count of 1 for inVlan ACLs
- 126 egress ACLs (outPort only):
  - 126 ACLs with 1 security ACE each (one of these ACLs can have 2 ACEs)

  This maximum implies a port member count of 1 for outPort ACLs.
- 766 ingress ACEs:

  Theoretical maximum of 766 implies 1 ingress ACL with 511 security ACEs and 255 QoS ACEs
  - Ingress ACEs supported: `(512 (security) - # of ACLs) + (256(QoS) - # of ACLs).`

  This maximum also implies a VLAN member count of 1 for an inVlan ACL.
- 252 egress ACEs:

  Theoretical maximum of 252 implies 1 egress ACL with 252 security ACEs
  - Egress ACEs supported: `253 - # of ACLs`.

  This maximum also implies a port member count of 1 for the outPort ACL.

VSP 8404C

The switch supports a maximum 3,070 non-IPv6 ingress ACEs, 2,047 IPv6 ingress ACEs, and 251 non-IPv6 egress ACEs.

IPv6 ingress and IPv6 egress QoS ACL/Filters are not supported. If you disable an ACL, the ACL state affects the administrative state of all of the ACEs within it.

The switch supports the following maximum limits for *ACL* scaling:

- 1,024 non-IPv6 ingress ACLs (inPort, inVlan, or InVSN):
  - 1,024 ACLs with 1 security ACE each OR
  - a combination based on the following rule:
    - `num of ACLs <= 1,024 AND (num of ACLs + Security ACEs) <= 2,048 AND (num of ACLs + QoS ACEs) <= 1,024`

  This maximum implies a VLAN member count of 1 for inVlan ACLs.
- 1,024 IPv6 ingress ACLs (inPort):
  - 1,024 IPv6 ACLs with 1 security ACE each OR

- a combination based on the following rule:
  - `num of IPv6 ACLs <= 1,024 AND (num of IPv6 ACLs + Security ACEs) <= 2,048`

- 126 non-IPv6 egress ACLs (outPort):
  - 126 ACLs with 1 Security ACE each OR
  - a combination based on the following rule:
    - `num ACLs <= 126 AND num ACLs + num security ACEs) <= 252`

  This maximum implies a port member counter of 1 for outPort ACLs.

The switch supports the following maximum limits for *ACE* scaling:

- 3,070 non-IPv6 ingress ACEs:

  The theoretical maximum implies the following configuration:
  - 1 non-IPv6 ingress ACL with 2,047 security ACEs and 1,023 QoS ACEs
  - a VLAN member count of 1 for inVlan ACLs
  - Non-IPv6 Ingress ACEs supported: `[2,048(security) - (num of ACLs)] + [1,024(QoS) - (num of ACLs)]`
- 2,047 IPv6 ingress ACEs:

  The theoretical maximum implies the following configuration:
  - 1 IPv6 ingress ACL with 2,047 security ACEs
  - IPv6 Ingress ACEs supported: `[2,048(security) - (num of ACLs)]`
- 251 non-IPv6 egress ACEs:

  The theoretical maximum implies the following configuration:
  - 1 egress ACL with 251 security ACEs
  - a port member count of 1 for outPort ACLs
  - Non IPv6 egress ACEs supported: `252 - (num egress ACLs)`

OAM and Diagnostics

Table 20: OAM and Diagnostics Maximums

Attribute	Product	Maximum number supported
EDM sessions	VSP 4450 Series	5
	VSP 7200 Series	5
	VSP 7400 Series	5

Table continues…

Attribute	Product	Maximum number supported
	VSP 8000 Series	5
FTP sessions (IPv4/IPv6)	VSP 4450 Series	8 total (4 for IPv4 and 4 for IPv6)
	VSP 7200 Series	8 total (4 for IPv4 and 4 for IPv6)
	VSP 7400 Series	8 total (4 for IPv4 and 4 for IPv6)
	VSP 8000 Series	8 total (4 for IPv4 and 4 for IPv6)
Rlogin sessions (IPv4/IPv6)	VSP 4450 Series	16 total (8 for IPv4 and 8 for IPv6)
	VSP 7200 Series	16 total (8 for IPv4 and 8 for IPv6)
	VSP 7400 Series	16 total (8 for IPv4 and 8 for IPv6)
	VSP 8000 Series	16 total (8 for IPv4 and 8 for IPv6)
SSH sessions (IPv4/IPv6)	VSP 4450 Series	8 total (any combination of IPv4 and IPv6)
	VSP 7200 Series	8 total (any combination of IPv4 and IPv6)
	VSP 7400 Series	8 total (any combination of IPv4 and IPv6)
	VSP 8000 Series	8 total (any combination of IPv4 and IPv6)
Telnet sessions (IPv4/IPv6)	VSP 4450 Series	16 total (8 for IPv4 and 8 for IPv6)
	VSP 7200 Series	16 total (8 for IPv4 and 8 for IPv6)
	VSP 7400 Series	16 total (8 for IPv4 and 8 for IPv6)
	VSP 8000 Series	16 total (8 for IPv4 and 8 for IPv6)
TFTP sessions (IPv4/IPv6)	VSP 4450 Series	2 total (any combination of IPv4 and IPv6)
	VSP 7200 Series	2 total (any combination of IPv4 and IPv6)
	VSP 7400 Series	2 total (any combination of IPv4 and IPv6)

Table continues…

Attribute	Product	Maximum number supported
	VSP 8000 Series	2 total (any combination of IPv4 and IPv6)
Mirrored ports (source)	VSP 4450 Series	49
	VSP 7200 Series	53 (up to 71 with channelization)
	VSP 7400 Series	31 (up to 125 with channelization) with Advanced Feature Bandwidth Reservation configured in Full Port mode
	VSP 8000 Series	83 (up to 95 with channelization)
Mirroring ports (destination)	VSP 4450 Series	4
	VSP 7200 Series	4
	VSP 7400 Series	4
	VSP 8000 Series	4
Fabric RSPAN Port mirror instances per switch (Ingress only)	VSP 4450 Series	Port mirror sessions can be mapped to 24 unique I-SID offsets for Ingress Mirror. Only one I-SID offset for Egress Mirror.
	VSP 7200 Series	Port mirror sessions can be mapped to 24 unique I-SID offsets for Ingress Mirror. Only one I-SID offset for Egress Mirror.
	VSP 7400 Series	Port mirror sessions can be mapped to 24 unique I-SID offsets for Ingress Mirror. Only one I-SID offset for Egress Mirror.
	VSP 8000 Series	Port mirror sessions can be mapped to 24 unique I-SID offsets for Ingress Mirror. Only one I-SID offset for Egress Mirror.
Fabric RSPAN Flow mirror instances per switch (Ingress only)	VSP 4450 Series	Filter ACL ACE sessions can be mapped to only 1 mirror I-SID offset.

Table continues…

Attribute	Product	Maximum number supported
	VSP 7200 Series	Filter ACL ACE sessions can be mapped to 24 unique I-SID offsets.
	VSP 7400 Series	Filter ACL ACE sessions can be mapped to 24 unique I-SID offsets.
	VSP 8000 Series	Filter ACL ACE sessions can be mapped to 24 unique I-SID offsets.
Fabric RSPAN Monitoring I-SIDs (network value)	VSP 4450 Series	1,000 Monitoring I-SIDs across SPB network
	VSP 7200 Series	1,000 Monitoring I-SIDs across SPB network
	VSP 7400 Series	1,000 Monitoring I-SIDs across SPB network
	VSP 8000 Series	1,000 Monitoring I-SIDs across SPB network
sFlow sampling limit	VSP 4450 Series	100 samples per second
	VSP 7200 Series	3,000 samples per second
	VSP 7400 Series	3,000 samples per second
	VSP 8000 Series	3,000 samples per second
IPFIX flows	VSP 4450 Series	n/a
	VSP 7200 Series	n/a
	VSP 7400 Series	20,000
	VSP 8000 Series	n/a

Virtualization Scaling

Note:

The scaling attributes in this section do not apply to the following products:

- VSP 4450 Series
- VSP 7200 Series
- VSP 8200 Series
- VSP 8400 Series

Table 21: Virtualization Maximums

Attribute	Product	Maximum number supported
Simultaneous Virtual Machines	VSP 7400 Series	5
CPU cores available to VMs	VSP 7400 Series	6
Memory available to VMs	VSP 7400 Series	12 GB
Storage available to VMs	VSP 7400 Series	100 GB
Total SRIOV vports available to VMs	VSP 7400 Series	16
Vports available to single VM	VSP 7400 Series	16

Fabric Scaling

This section lists the fabric scaling information.

Table 22: Fabric Maximums

Attribute	Product	vIST configuration	vIST not configured
Number of SPB regions	VSP 4450 Series	1	1
	VSP 7200 Series	1	1
	VSP 7400 Series	1	1
	VSP 8000 Series	1	1
Number of B-VIDs	VSP 4450 Series	2	2
	VSP 7200 Series	2	2
	VSP 7400 Series	2	2
	VSP 8000 Series	2	2
Maximum number of Physical and Logical (Fabric Extend) NNI interfaces/adjacencies	VSP 4450 Series	255	255
	VSP 7200 Series	255	255
	VSP 7400 Series	255	255
	VSP 8000 Series	255	255
SPBM enabled nodes per area (BEB + BCB)	VSP 4450 Series	550	550
	VSP 7200 Series	800	800
	VSP 7400 Series	2,000	2,000
	VSP 8000 Series	800	800
Number of BEBs this node can share services with (Layer 2 VSNs, Layer 3 VSNs, E-Tree, Multicast, Transparent Port UNI).	VSP 4450 Series	500	500
	VSP 7200 Series	500	500
	VSP 7400 Series	2,000	2,000

Table continues…

Attribute	Product	vIST configuration	vIST not configured
Note: vIST clusters are counted as 3 nodes. Each Fabric Extend IS-IS adjacency or VXLAN remote VTEP reduces this number by 1.	VSP 8000 Series	500	500
Maximum number of vIST/IST clusters this node can share I-SIDs with	VSP 4450 Series	500	500
	VSP 7200 Series	330	330
	VSP 7400 Series	2,000	2,000
	VSP 8000 Series	330	330
Layer 2 MAC table size (with SPBM)	VSP 4450 Series	16,000	16,000
	VSP 7200 Series	112,000	112,000
	VSP 7400 Series	80,000	80,000
	VSP 8000 Series	112,000	112,000
I-SIDs supported	VSP 4450 Series	See Number of I-SIDs supported on page 60	See Number of I-SIDs supported on page 60
	VSP 7200 Series	See Number of I-SIDs supported on page 60	See Number of I-SIDs supported on page 60
	VSP 7400 Series	See Number of I-SIDs supported on page 60	See Number of I-SIDs supported on page 60
	VSP 8000 Series	See Number of I-SIDs supported on page 60	See Number of I-SIDs supported on page 60
Maximum number of Layer 2 VSNs per switch	VSP 4450 Series	1,000	1,000
	VSP 7200 Series	4,059	4,059
	VSP 7400 Series	4,000	4,000
	VSP 8000 Series	4,059	4,059
Maximum number of Switched UNI I-SIDs per switch	VSP 4450 Series	See Number of I-SIDs supported on page 60	See Number of I-SIDs supported on page 60
	VSP 7200 Series	See Number of I-SIDs supported on page 60	See Number of I-SIDs supported on page 60
	VSP 7400 Series	See Number of I-SIDs supported on page 60	See Number of I-SIDs supported on page 60

Table continues…

Attribute	Product	vIST configuration	vIST not configured
	VSP 8000 Series	See Number of I-SIDs supported on page 60	See Number of I-SIDs supported on page 60
Maximum number of Transparent Port UNIs per switch	VSP 4450 Series	48	48
	VSP 7200 Series	54 (up to 72 with channelization)	54 (up to 72 with channelization)
	VSP 7400 Series	32 (up to 125 with channelization) with Advanced Feature Bandwidth Reservation configured in Full Port mode	32 (up to 125 with channelization) with Advanced Feature Bandwidth Reservation configured in Full Port mode
	VSP 8000 Series	84 (up to 96 with channelization)	84 (up to 96 with channelization)
Maximum number of E-Tree PVLAN UNIs per switch	VSP 4450 Series	200	200
	VSP 7200 Series	200	200
	VSP 7400 Series	200	200
	VSP 8000 Series	VSP 8404C = 400 Other VSP 8000 Series platforms = 200	VSP 8404C = 400 Other VSP 8000 Series platforms = 200
Maximum number of Layer 3 VSNs per switch See VRF Scaling on page 62.	VSP 4450 Series	128 including mgmt VRF and GRT	128 including mgmt VRF and GRT
	VSP 7200 Series	256 including mgmt VRF and GRT	256 including mgmt VRF and GRT
	VSP 7400 Series	256 including mgmt VRF and GRT	256 including mgmt VRF and GRT
	VSP 8000 Series	256 including mgmt VRF and GRT	256 including mgmt VRF and GRT
Maximum number of SPB Layer 2 multicast UNI I-SIDs	VSP 4450 Series	See Number of I-SIDs supported on page 60	See Number of I-SIDs supported on page 60
	VSP 7200 Series	See Number of I-SIDs supported on page 60	See Number of I-SIDs supported on page 60
	VSP 7400 Series	See Number of I-SIDs supported on page 60	See Number of I-SIDs supported on page 60

Table continues…

Attribute	Product	vIST configuration	vIST not configured
	VSP 8000 Series	See Number of I-SIDs supported on page 60	See Number of I-SIDs supported on page 60
Maximum number of SPB Layer 3 multicast UNI I-SIDs	VSP 4450 Series	Maximum 1,000 for a BEB: Due to internal resource sharing IP Multicast scaling depends on network topology. Switch will issue warning when 85 and 90% of available resources are reached.	
	VSP 7200 Series	Maximum 6,000 for a BEB: Due to internal resource sharing IP Multicast scaling depends on network topology. Switch will issue warning when 85 and 90% of available resources are reached.	
	VSP 7400 Series	Maximum 6,000 for a BEB: Due to internal resource sharing IP Multicast scaling depends on network topology. Switch will issue warning when 85 and 90% of available resources are reached.	
	VSP 8000 Series	Maximum 6,000 for a BEB: Due to internal resource sharing IP Multicast scaling depends on network topology. Switch will issue warning when 85 and 90% of available resources are reached.	
Maximum number of FA ISID/VLAN assignments per port	VSP 4450 Series	94	94
	VSP 7200 Series	94	94
	VSP 7400 Series	94	94
	VSP 8000 Series	94	94
Maximum number of IP multicast S,Gs when operating as a BCB	VSP 4450 Series	1,000	1,000
	VSP 7200 Series	16,000	16,000
	VSP 7400 Series	50,000	50,000
	VSP 8000 Series	16,000	16,000

Number of I-SIDs Supported for the Number of Configured IS-IS Interfaces and Adjacencies (NNIs)

The number of I-SIDs supported depends on the number of IS-IS interfaces and adjacencies (NNIs) configured.

The following table shows the number of UNI I-SIDs supported per BEB. UNI I-SIDs are used for Layer 2 VSN, Layer 3 VSN, Transparent-UNI, E-Tree, Switched-UNI and S, G for Multicast.

Number of IS-IS interfaces (NNIs)	Product	I-SIDs with vIST configured on the platform	I-SIDs without vIST configured on the platform
4	VSP 4450 Series	1,000	1,000
	VSP 7200 Series	4,000	4,000
	VSP 7400 Series	4,000	4,000
	VSP 8000 Series	4,000	4,000
6	VSP 4450 Series	1,000	1,000
	VSP 7200 Series	3,500	4,000
	VSP 7400 Series	3,500	4,000
	VSP 8000 Series	3,500	4,000
10	VSP 4450 Series	650	1,000
	VSP 7200 Series	2,900	4,000
	VSP 7400 Series	2,900	4,000
	VSP 8000 Series	2,900	4,000
20	VSP 4450 Series	350	700
	VSP 7200 Series	2,000	4,000
	VSP 7400 Series	2,000	4,000
	VSP 8000 Series	2,000	4,000
48	VSP 4450 Series	n/a	n/a
	VSP 7200 Series	1,000	2,000
	VSP 7400 Series	1,000	2,000
	VSP 8000 Series	1,000	2,000
72	VSP 4450 Series	n/a	n/a
	VSP 7200 Series	750	1,500
	VSP 7400 Series	750	1,500
	VSP 8000 Series	750	1,500
100	VSP 4450 Series	n/a	n/a
	VSP 7200 Series	550	1,100
	VSP 7400 Series	550	1,100
	VSP 8000 Series	550	1,100
128	VSP 4450 Series	n/a	n/a
	VSP 7200 Series	450	900
	VSP 7400 Series	450	900
	VSP 8000 Series	450	900
250	VSP 4450 Series	n/a	n/a
	VSP 7200 Series	240	480

Table continues…

Number of IS-IS interfaces (NNIs)	Product	I-SIDs with vIST configured on the platform	I-SIDs without vIST configured on the platform
	VSP 7400 Series	240	480
	VSP 8000 Series	240	480

Interoperability Considerations for IS-IS External Metric

BEBs running VOSS 5.0 can advertise routes into IS-IS with the metric type as external. They can also correctly interpret route advertisements with metric type external received via IS-IS. In an SPB network with a mix of products running different versions of software releases, you must take care to ensure that turning on the ability to use metric-type external does not cause unintended loss of connectivity.

Note the following before turning on IS-IS external metric if the SPB network has switches running a release prior to VOSS 5.0:

- There are no special release or product type implications if the switch does not have IP Shortcuts or Layer 3 VSN enabled. For example, this applies to Layer 2 only BEBs and BCBs.
- There are no special release or product type implications if the Layer 3 VSN in which routes are being advertised with a metric-type of external is not configured on the switch.
- If a switch running a VOSS release that is prior to VOSS 5.0 but VOSS 4.2.1 or later, it will treat all IS-IS routes as having metric-type internal, regardless of the metric-type (internal or external) used by the advertising BEB in its route advertisement.
- Switches running VSP 9000 release 4.1.0.0 or later will treat all IS-IS routes as having metric-type internal, regardless of the metric-type (internal or external) used by the advertising BEB in its route advertisement.
- Switches running VOSS releases prior to 4.2.1.0 may not correctly install IS-IS routes in a Layer 3 VSN if any routes advertised with metric-type external are advertised in that Layer 3 VSN by other BEBs in the network. Layer 3 VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to the GRT.
- Switches running VSP 9000 releases prior to 4.1.0.0 may not correctly install IS-IS routes in a Layer 3 VSN if any routes advertised with metric-type external are advertised in that Layer 3 VSN by other BEBs in the network. Layer 3 VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to GRT.
- Switches running any ERS 8800 release may not correctly install IS-IS routes in a Layer 3 VSN if any routes advertised with metric-type external are advertised in that Layer 3 VSN by other BEBs in the network. Layer 3 VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to GRT.

Recommendations

This section provides recommendations that affect feature configuration.

Pay special attention to the expected scaling of routes in the network and the number of OSPF neighbors in a single VRF when you select configuration values for the **`isis l1-hellointerval`** and **`isis l1-hello-multiplier`** commands on IS-IS interfaces. The default values for these commands work well for most networks, including those using moderately-scaled routes.

VSP 7200 Series, VSP 7400 Series, and VSP 8000 Series

The default values work well for 16,000 routes and 64 OSPF neighbors in a single VRF. However, in highly-scaled networks, you may need to configure higher values for these commands.

For example, if the total number of non IS-IS routes on a given BEB exceeds 16,000 in combination with approximately 128 OSPF neighbors in a single VRF, you should configure a value of 12 for **`isis l1-hellomultiplier`**, instead of using the default value of 3.

VSP 4450 Series

If the total number of non IS-IS routes on a given BEB exceeds 25,000 in combination with approximately 60,000 IS-IS routes that the BEB receives from other BEBs in the network, you should configure a value of 12 for **`isis l1-hellomultiplier`**, instead of using the default value of 3.

VRF Scaling

By default, the system reserves VLAN IDs 4060 to 4094 for internal use.

If you enable both the VRF scaling and the SPBM mode boot configuration flags, the system reserves additional VLAN IDs (3500 to 3998) for internal use.

By default, VRF scaling is disabled and SPBM mode is enabled.

Chapter 6: Important Notices

Unless specifically stated otherwise, the notices in this section apply to all VOSS platforms.

100BASE-FX Support on VSP 4000 Series

VSP 4000 Series supports 100BASE-FX transceivers on the VSP 4450GSX or VSP 4850 Series models in SFP ports only. These models do not support 100BASE-FX in SFP+ ports.

AES-GCM SSH Connection with Open SSH

Switch side encryption and authentication type must be set to the AES-GCM-128/256 methods and needs at least one hmac method in the authentication list in addition for the connection to work.

Auto Negotiation Settings

VOSS 4.1 and later software requires the same auto negotiation settings on link partners to avoid incorrect declaration of link status. Mismatched settings can cause the links to stay down as well as unpredictable behavior. Ensure the auto negotiation settings between local ports and their remote link partners match before upgrading software to VOSS 4.1 or later.

dos-chkdsk

If at the end of the **dos-chkdsk WORD<1-99>** command output you see the following choice:

```
    1) Correct
    2) Don't correct
```

Then, you should run the **dos-chkdsk WORD<1-99> repair** command.

Fabric Attach Interoperability Notes

For Fabric Attach to operate between a VOSS platform and an ERS device, the ERS device must meet minimum software requirements. The following tables identify the minimum GA software releases required to build an FA solution.

Table 23: Extending Fabric using Static FA Proxy Configuration (ISID/VLAN is Manually Configured on FA Proxy)

FA Server		FA Proxy	
Product	**Minimum release**	**Product**	**Minimum release**
VSP 4000 Series	5.0.0.0	ERS 5900	7.0.1
VSP 7200 Series		ERS 5600	6.6.3
VSP 7400 Series	8.0	ERS 4800	5.9.2
VSP 8200 Series	5.0.0.0	ERS 4500	5.7.3
VSP 8400 Series			

Table 24: Extending Fabric to FA Clients by Using FA Proxy

FA Server		FA Proxy		FA Policy	FA Client	
Product	**Minimum release**	**Product**	**Minimum release**		**Product**	**Minimum release**
VSP 4000 Series	5.0.0.0	ERS 5900	7.0.1	IDE Release 9.1* (See Note)	AP9100	7.2.5
VSP 7200 Series		ERS 5600	6.6.3			
VSP 7400 Series	8.0	ERS 4800	5.9.2			
VSP 8200 Series	5.0.0.0	ERS 4500	5.7.3			
VSP 8400 Series						

Note:

* Required for AP9100 FA Client. IDE sends FA ISID/VLAN assignment request by using FA Proxy to VOSS FA Server.

IKEv2 Digital Certificate Support with Strong Swan

Strong Swan server must be customized to get IKEv2 Digital Certificate connection between switch and server for RFCs that Strong Swan is compliant and switch is not. This includes SHA256 signing check, IPv6 identifier check and others.

Feature Licensing

The VOSS platforms support a licensing model that includes Base and Premier licenses. The Base License, which is included with the purchase of the switch, enables the basic networking capabilities of the device. You can purchase Premier Licenses separately to enable advanced features on the switch.

Premier Licenses enable advanced features not available in the Base License. The following table provides information on the Premier Licenses that the switch supports.

License type	Supported features
Premier License	• Fabric Connect Layer 3 Virtual Services Networks (VSNs) • DvR Controller • VXLAN Gateway • Greater than 24 VRFs • Greater than 16 BGP peers • Extreme Insight (on supporting hardware)
Premier with MACsec License	• Fabric Connect Layer 3 Virtual Services Networks (VSNs) • DvR Controller • VXLAN Gateway • Greater than 24 VRFs • Greater than 16 BGP peers • Extreme Insight (on supporting hardware) • IEEE 802.1AE MACsec (on supporting hardware)

For information about licensing including order codes and how to load a license file, see Administering VOSS.

show vlan remote-mac-table Command Output

The output for the **`show vlan remote-mac-table`** command can be different than what appears for the same command on VSP 9000.

Because all MinM packets that originate from the IST switch use the virtual B-MAC as the source BMAC, the remote BEB learns the C-MAC against the virtual B-MAC. Because the remote BEB uses the shortest path to the virtual B-MAC, the remote BEB can show the IST peer as a tunnel in the show vlan remote-mac-table command output.

Supported Browsers

Use the following recommended browser versions to access Enterprise Device Manager (EDM):

- Microsoft Edge 41.16299.15.0
- Microsoft Internet Explorer 11
- Mozilla Firefox 58.0.2
- Google Chrome 64.0.3282.140

Note:

The following earlier browser versions can be used to access EDM (although not recommended):

- Microsoft Internet Explorer 9 and 10
- Mozilla Firefox 37 through 57

System Name Prompt vs. IS-IS Host Name

Beginning with VOSS 6.1.2, the software no longer allows spaces in the system name prompt, but it still allows spaces in the IS-IS host name. When you upgrade, the software replaces spaces in the system name with underscores while leaving the IS-IS host name unchanged.

Feature Differences

Extreme Networks has implemented feature parity between the VOSS platforms in all but a few exceptions. Some features are supported on one platform and not another to maintain compatibility with previous releases. In other cases, the difference is between of the role of the switch in the network.

The following table summarizes the feature differences between the platforms in this release.

Feature	VSP 4000 Series	VSP 7200 Series	VSP 7400 Series	VSP 8000 Series
Advanced Feature Bandwidth Reservation	Not required	Not required	Supported	Not required

Table continues…

Feature	VSP 4000 Series	VSP 7200 Series	VSP 7400 Series	VSP 8000 Series
CFM CMAC for the CVLAN	Supported	Not supported	Not supported	Not supported
Channelization of 40 Gbps ports	Not applicable	Supported	Supported	Supported
Channelization of 100 Gbps ports	Not applicable	Not applicable	Supported	Not applicable
DvR Controller	Not supported	Supported	Supported	Supported
Dynamic Nickname Assignment	Not supported on VSP 4850 Series	Supported	Not Supported	Supported
Energy Saver	Supported	VSP 7254XTQ only	Not applicable	VSP 8400 Series ESMs with copper interfaces only
Extreme Insight	Not supported	Not supported	Supported	Not supported
Fabric RSPAN	Flow-based Mirroring into single ISID only	Supported	Supported	Supported
FDB protected by port (MAC security limit-learning)	Supported	Not supported	Not supported	Not supported
Ingress Dual Rate Port Policers	Supported	Not supported	Not supported	Not supported
IPFIX	Not supported	Not supported	Supported	Not supported
Layer 2 Video Surveillance install script	Supported	Supported	Not supported	Not supported
Layer 3 Video Surveillance install script (formerly called Endura script)	Supported	Not supported	Not supported	Not supported
Multicast Route Statistics for IPv4 and IPv6	Not supported	Supported	Supported	Supported
NLB Unicast and Multicast	Not supported	Supported	Supported	Supported
PoE/PoE+ Allocation Using LLDP	Supported on VSP 4850GTS-PWR+ and VSP 4450GTX-HT-PWR+	Not supported	Not supported	Not supported
Port licensing	Not supported	Applies to Port licensed VSP 7254XSQ fiber	Not supported	Not supported

Table continues…

Feature	VSP 4000 Series	VSP 7200 Series	VSP 7400 Series	VSP 8000 Series
		switch and VSP 7254XTQcopper switch		
QoS	Supported	Supported with exceptions: • Classification does not have routed packet classification • No ingress policer- Uses ingress port rate limiting instead	Supported with exceptions: • Classification does not have routed packet classification • No ingress policer or ingress port rate limiting	Supported with exceptions: • Classification does not have routed packet classification • No ingress policer- Uses ingress port rate limiting instead
sFlow	Reduced sampling rate	Supported	Supported	Supported
Software licensing (Premier)	Supports licenses generated from the Avaya Data Licensing Portal and the Product Licensing & Delivery System (PLDS) Supports licenses with Extreme signatures	Supports licenses generated from the Avaya Product Licensing & Delivery System (PLDS) Supports licenses with Extreme signatures	Supports licenses with Extreme signatures	Supports licenses generated from the Avaya Product Licensing & Delivery System (PLDS) Supports licenses with Extreme signatures
SPM-PIM GW Controller	Not supported on VSP 4850 Series	Supported	Supported	Supported
Use of Open Networking Adapter for Fabric Extend	Required	Not required	Not required	Not required
VXLAN Gateway	Not supported	Supported	Supported	Supported
Zero Touch Fabric configuration	Not supported on VSP 4850 Series	Supported	Not Supported	Supported

VSP 4000 Series Connecting to an ERS 8800 Interoperability Notes

- For customers running ERS 8800 version 7.1.x:
  - The minimum software release is 7.1.3.1, however the recommended ERS 8800 software release is 7.1.5.4 or later.

  - On switches using 8612 XLRS or 8812XL modules for the links connecting to the VSP 4000 Series, the minimum software version is 7.1.5.4.
  - The “spbm version” on the ERS 8800 must be “802.1aq”.
- For customers running ERS 8800 version 7.2.x:
  - The minimum software release is 7.2.0.2, however the recommended ERS 8800 software release is 7.2.1.1 or later.
  - On switches using 8612 XLRS or 8812XL modules for the links connecting to the VSP 4000 Series switch, the minimum software version is 7.2.1.1.
- Diffserv is enabled in the VSP 4000 Series port settings, and is disabled in the ERS 8800 port settings, by default.

VSP 4000 Series Notes on Combination Ports

When the VSP 4000 Series is reset, the peer connections for all ports, including combination ports 47 and 48 on VSP 4450GTX-HT-PWR+, will transition down. During the reset, the fiber ports remain down, but only the copper ports 47 and 48 come up periodically throughout the reset. The copper ports 47 and 48 come up approximately 15 seconds into the reset, remain up for approximately 60 seconds, and then transition down until the boot sequence is complete and all ports come back up.

The following is an example of the status of the combination ports during reset.

```
CP1 [03/18/70 09:55:35.890] 0x0000c5e7 00300001.238 DYNAMIC SET GlobalRouter HW INFO Link
Down(1/47)
CP1 [03/18/70 09:55:35.903] 0x0000c5e7 00300001.239 DYNAMIC SET GlobalRouter HW INFO Link
Down(1/48)
CP1 [03/18/70 09:55:49.994] 0x0000c5ec 00300001.239 DYNAMIC CLEAR GlobalRouter HW INFO
Link Up(1/48)
CP1 [03/18/70 09:55:50.322] 0x0000c5ec 00300001.238 DYNAMIC CLEAR GlobalRouter HW INFO
Link Up(1/47)
CP1 [03/18/70 09:56:43.131] 0x0000c5e7 00300001.238 DYNAMIC SET GlobalRouter HW INFO Link
Down(1/47)
CP1 [03/18/70 09:56:43.248] 0x0000c5e7 00300001.239 DYNAMIC SET GlobalRouter HW INFO Link
Down(1/48)
```

Cabled Connections for Both Copper and Fiber Ports

The following limitations apply when the combination ports have cabled connections for both the copper and fiber ports.

Do not use the fiber port and do not insert an SFP into the optical module slot in the following situations:

- a copper speed setting of either 10M or 100M is required
- a copper duplex setting of half-duplex is required

Note:

These limitations apply only when auto-negotiation is disabled. To avoid this limitation, use auto-negotiation to determine the speed to 10/100/1000 and to determine the duplex.

The 100M-FX SFP requires auto-negotiation to be disabled. Therefore, auto-negotiation will also be disabled for the copper port. Configure the peer switch to disable auto-negotiation.

Chapter 7: Known Issues and Restrictions

This section details the known issues and restrictions found in this release. Where appropriate, use the workarounds provided.

Known Issues

This section identifies the known issues in this release.

Known Issues for VOSS 8.0

Issue number	Description	Workaround
-	HTTPS connection fails for CA-signed certificate with certificate inadequate type error on FF.	Ensure End-Entity, Intermediate CA and Root CA certificates are all SHA256 based and RSA2048 key signed, and Extended key usage field is set to TLS webserver Auth only for subject and root. For intermediate, it must be set with other required bits to avoid this issue. Add the root, intermediate CAs in the trust store of the browser for accessing the EDM with HTTPS.
-	VRF provisioning is restricted to 127 VRFs on VSP 4000 Series.	None.
VOSS-1265	On the port that is removed from a T-UNI LACP MLT, non T-UNI configuration is blocked as a result of T-UNI consistency checks.	When a port is removed from a T-UNI LACP MLT, the LACP key of the port must be set to default.
VOSS-1278	SLA Mon tests fail (between 2% and 8% failure) between devices when you have too many agents involved with scaled configurations.	This happens only in a scaled scenario with more than seven agents, otherwise the failure does not occur. The acceptable failure percentage is 5%, but you may see failures of up to 8%.
VOSS-1280	The following error message occurs when performing shutdown/no-shutdown commands continuously: `IO1 [05/02/14 06:59:55.178:UTC] 0x0011c525`	None. When this issue occurs, the port in question can go down, then performs a shutdown/no-shutdown of the port to bring it up and resumes operation.

Table continues…

Issue number	Description	Workaround
	`00000000 GlobalRouter COP-SW ERROR vsp4kTxEnable Error changing TX disable for SFP module: 24, code: -8`	
VOSS-1284	On a fresh boot, peer ports connected to ports 1/49 and 1/50 bounce and can cause additional transitions in the network.	None.
VOSS-1285	CAKs are not cleared after setting the device to factory-default.	None. Currently this is the default behavior and does not affect functionality of the MACsec feature.
VOSS-1288	Shutting down the T1 link from one end of the link does not shut down the link at the remote end. You may experience traffic loss if the remote side of the link is not shut down.	This issue occurs only when a T1 SFP link from one end is shutdown. Enable a dynamic link layer protocol such as LACP or VLACP on both ends to shut the remote end down too. As an alternative, administratively disable both ends of the T1 SFP link to avoid the impact.
VOSS-1289	On a MACsec-enabled port, you can see delayed packets when the MACsec port is kept running for more than 12 hours. This delayed packet counter can also increment when there is complete reordering of packets so that the application might receive a slow response. But in this second case, it is a marginal increase in the packet count, which occurs due to PN mismatch sometimes only during Key expiry, and does not induce any latency.	None.
VOSS-1309	You cannot use EDM to issue **`ping`** or **`traceroute`** commands for IPv6 addresses.	Use CLI to initiate **`ping`** and **`traceroute`** commands.
VOSS-1310	You cannot use EDM to issue **`ping`** or **`traceroute`** commands for IPv4 addresses.	Use CLI to initiate **`ping`** and **`traceroute`** commands.
VOSS-1312	On the 40-gigabit ports, the small metallic fingers that surround the ports are fragile and can bend out of shape during removal and insertion of the transceivers. When the fingers are bent, they prevent the insertion of the QSFP+ transceiver.	Insert the QSFP+ carefully. If the port gets damaged, it needs to be repaired.
VOSS-1335	In an IGMP snoop environment, after dynamically downgrading the IGMP version to version 2 (v2), when you revert	Use a v3 interface as querier in a LAN segment that has snoop-enabled v2 and v3 interfaces.

Table continues…

Issue number	Description	Workaround
	back to version 3 (v3), the following is observed: • The multicast traffic does not flow. • The sender entries are not learned on the local sender switch. • The Indiscard packet count gets incremented on the **`show int gig error`** statistics command.	
VOSS-1340	From EDM, you cannot perform a Layer 2 IP ping for an IPv6 address. EDM displays the following error: `No next Hop address found for ip address provided`	Use the CLI to perform a Layer 2 IP ping.
VOSS-1344	In EDM, you cannot select multiple 40 gigabit ports or a range of ports that includes 40 gigabit ports to graph or edit. You need to select them and edit them individually.	None.
VOSS-1348	In the COM EDM Plugin command, the Layer 2 Traceroute IPv6 does not work properly and displays the error: `No Such Name`.	Use the CLI to initiate the Layer 2 Traceroute for IPv6.
VOSS-1349	On EDM, the port LED for channelized ports only shows the status of sub-port #1, but not the rest of the sub-ports. When you remove sub-port #1, and at least one other sub-port is active and online, the LED color changes to amber, when it should be green because at least one other sub-ports is active and online. The LED only shows the status of sub-port #1.	None.
VOSS-1354	An intermittent link-flap issue can occur in the following circumstance for the copper ports. If you use a crossover cable and disable auto-negotiation, the port operates at 100 Mbps. A link flap issue can occur intermittently and link flap detect will shutdown the port.	Administratively shutdown, and then reenable the port. Use auto-negotiation. Disabling auto-negotiation on these ports is not a recommended configuration.
VOSS-1358	Traffic is forwarded to IGMP v2 SSM group, even after you delete the IGMP SSM-map entry for the group.	If you perform the delete action first, you can recreate the SSM-map record, and then disable the SSM-map record. The disabled SSM-map record causes the receiver to timeout because any subsequent membership reports that arrive

Table continues…

Issue number	Description	Workaround
		and match the disabled SSM-map record are dropped. You can delete the SSM-map record after the receivers time out.
VOSS-1359	The 4 byte AS confederation identifier and peers configuration are not retained across a reboot. This problem occurs when 4 Byte AS is enabled with confederation.	Reconfigure the 4 byte AS confederation identifier and peers on the device, and reboot.
VOSS-1360	After you enable enhanced secure mode, and log in for the first time, the system prompts you to enter a new password. If you do not meet the minimum password requirements, the following system output message appears: `Password should contain a minimum of 2 upper and lowercase letters, 2 numbers and 2 special characters like !@#$%^*(). Password change aborted. Enter the New password:` The system output message does not display the actual minimum password requirements you need to meet, which are configured on your system. The output message is an example of what the requirements may need to meet. The actual minimum password requirements you need to meet are configured on your system by the administrator.	None.
VOSS-1367	The router ospf entry always appears in the configuration file regardless of whether OSPF is configured. This line does not perform any configuration and has no impact on the running software.	None.
VOSS-1368	When you use Telnet or SSH to connect to the switch, it can take up to 60 seconds for the login prompt to appear. However, this situation is very unlikely to happen, and it does not appear in a standard normal operational network.	Do not provision DNS servers on a switch to avoid this issue altogether.
VOSS-1370	If you configure egress mirroring on NNI ports, you do not see the MAC-in-MAC header on captured packets.	Use an Rx mirror on the other end of the link to see the packets.
VOSS-1371	A large number of IPv6 VRRP VR instances on the same VLAN can cause high CPU utilization.	Do not create more than 10 IPv6 VRRP VRs on a single VLAN.

Table continues…

Issue number	Description	Workaround
VOSS-1389	If you disable IPv6 on one RSMLT peer, the switch can intermittently display `COP-SW ERROR` and `RCIP6 ERROR` error messages. This issue has no impact.	None.
VOSS-1390	If you delete the SPBM configuration and re-configure SPBM using the same nickname but a different IS-IS system ID without rebooting, the switch displays an error message.	Reboot the switch after you delete the SPBM configuration.
VOSS-1402	You cannot use EDM to configure SSH rekey, or to enable or disable SFTP.	Use CLI to configure SSH rekey, and to enable or disable SFTP.
VOSS-1403	EDM displays the user name as Admin, even though you login using a different user name.	None.
VOSS-1404	You cannot use EDM to view the IPv6 DHCP relay counters.	Use CLI to view the IPv6 DHCP relay counters.
VOSS-1406	When you re-enable insecure protocols in the CLI SSH secure mode, the switch does not display a warning message.	None.
VOSS-1418	EDM displays the IGMP group entry that is learned on a vIST MLT port as TX-NNI.	Use CLI to view the IGMP group entry learned on a vIST MLT port.
VOSS-1428	When port-lock is enabled on the port and re-authentication on the EAP client fails, the port is removed from the RAIUS-assigned VLAN. This adds the port to the default VLAN and displays an error message. This issue has no impact.	The error message is incorrect and can be ignored.
VOSS-1433	When you manually enable or disable IS-IS on 40 Gbps ports with CR4 direct attach cables (DAC), the port bounces once.	Configure IS-IS during the maintenance period. Bring the port down, configure the port and then bring the port up.
VOSS-1438	In a rare scenario in Simplified vIST configuration when vIST state is toggled immediately followed by vIST MLT ports are toggled, one of the MLT ports will go into blocking state resulting in failure to process data packets hashing to that link.	Before enabling vIST state ensure all vIST MLT ports are shut and re-enabled after vIST is enabled on the DUT.
VOSS-1440 VOSS-1441	When you configure a scaled Layer 3 VSN (24 Layer 3 VSN instances), route leaking from GRT to VRF on the local DUT does not happen. The switch displays an incorrect error message: `Only 24 Layer 3 VSNs can be configured.`	None.
VOSS-1459	When you use Fabric Extend over IP (FE-IP) and Fabric Extend over Layer 2 VLAN	Do not change the default ingress and egress .1p maps when using Fabric

Table continues…

Issue number	Description	Workaround
VOSS-1463 VOSS-1471	(FE-VID) solution, if you change the ingress and egress .1p map, packets may not follow correct internal QoS queues for FE tunnel to FE tunnel, or FE tunnel to regular NNI traffic.	Extend. With default ingress and egress . 1p maps, packets follow the correct internal QoS when using the Fabric Extend feature.
VOSS-1473	If the I-SID associated with a Switched UNI or Fabric Attach port does not have a platform VLAN association and you disable Layer 2 Trusted, then the non IP traffic coming from that port does not take the port QoS and still uses the .1p priority in the packet.	None.
VOSS-1530	If you improperly close an SSH session, the session structure information does not clear and the client can stop functioning.	Disable and enable SSH.
VOSS-1560	If you apply an ipv6-out-route-map on a BGP peer to filter a particular IPv6 prefix range with a match network condition, it does not filter the full prefix range.	Configure the incoming policy to filter incoming advertised routes on BGP+ peers.
VOSS-1584	The **`show debug-file all`** command is missing.	None.
VOSS-1585	The system does not generate a log message, either in the log file or on screen, when you run the **`flight-recorder`** command.	None.
VOSS-1608	If you use an ERS 4850 FA Proxy with a VOSS FA Server, a mismatch can exist in the show output for tagged management traffic. The ERS device always sends traffic as tagged. The VOSS FA Server can send both tagged and untagged. For untagged, the VOSS FA Server sends VLAN ID 4095 in the management VLAN field of the FA element TLV. The ERS device does not recognize this VLAN ID and so still reports the traffic as tagged.	There is no functional impact.
VOSS-1706	EAPOL: Untagged traffic is not honoring the port QOS for Layer 2 trusted/ Layer 3 untrusted. This issue is only seen on EAPOL-enabled ports.	None.
VOSS-2014	IPV6 MLD Group is learned for Link-Local Scope Multicast Addresses. This displays additional entries in the Multicast routing tables.	None.

Table continues…

Issue number	Description	Workaround

VOSS-2033	The following error messages appear when you use the **shutdown** and **no shutdown** commands on the MLT interface with ECMP and BGP+ enabled:
	`CP1 [01/23/16 11:10:16.474:UTC] 0x00108628 00000000 GlobalRouter RCIP6 ERROR rcIpReplaceRouteNotifyIpv6:FAIL ReplaceTunnelRec conn_id 2`
	`CP1 [12/09/15 12:27:02.203:UTC] 0x00108649 00000000 GlobalRouter RCIP6 ERROR ifyRpcOutDelFibEntry: del FIB of Ipv6Route failed with 0: ipv6addr: 201:6:604:0:0:0:0:0, mask: 96, nh: 0:0:0:0:0:0:0:0 cid 6657 owner BGP`
	`CP1 [12/09/15 12:20:30.302:UTC] 0x00108649 00000000 GlobalRouter RCIP6 ERROR ifyRpcOutDelFibEntry: del FIB of Ipv6Route failed with 0: ipv6addr: 210:6:782:0:0:0:0:0, mask: 96, nh: fe80:0:0:0:b2ad:aaff:fe55:5088 cid 2361 owner OSPF`
		Disable the alternate path.

VOSS-2036	IPsec statistics for the management interface do not increment for inESPFailures or InAHFailures.	None.
VOSS-2117	If you configure static IGMP receivers on an IGMPv3 interface and a dynamic join and leave are received on that device from the same destination VLAN or egress point, the device stops forwarding traffic to the static receiver group after the dynamic leave is processed on the device. The end result is that the IGMP static groups still exist on the device but traffic is not forwarded.	Disable and re-enable IGMP Snooping on the interface.
VOSS-2128	EAP Security and Authentication EDM tabs display additional information with internal values populated, which is not useful for the end user.	There is no functional impact. Ignore the additional information in EDM. Use the CLI command **show eapol port interface** to see port status.
VOSS-2207	You cannot configure an SMTP server hostname that begins with a digit. The	None.

Table continues…

Issue number	Description	Workaround
	system displays the following error: `Error: Invalid IP Address or Hostname for SMTP server`	
VOSS-2208	While performing CFM Layer 2 traceroute between two BEBs via a transit BCB, the transit BCB hop is not seen, if the transit BCB has ISIS adjacencies over FE l3core with both source BEB and destination BEB.	None.
VOSS-2253	Trace level command does not list module IDs when '**?**' is used.	To get the list of all module IDs, type **`trace level,`** and then press **`Enter.`**
VOSS-2270	The packet internal CoS is derived incorrectly for packets sourced from a brouter port when the CoS should be derived from the port level QoS. The following list identifies scenarios that derive the internal CoS from the port QoS: • Untagged non-IP packet • Untagged IP packet, and the source port is Layer 3 untrusted • Tagged non-IP packet and the source port is Layer 2 untrusted • Tagged IP packet and the source port is Layer 3 untrusted and Layer 2 untrusted	Use the port default QoS configuration for the brouter port. The port default configuration is Layer 2 trusted and Layer 3 trusted, and under this configuration, only the first scenario in the list is still an issue. The other scenarios do not occur.
VOSS-2279	When an IPv6 neighbor device boots, the following error message occurs in the peer device console: `GlobalRouter COP-SW ERROR ercdProcIpv6RouteMsg: Failed to Delete IPV6 Record - Ip: fe80:0:0:8dc:b2ad:aaff:fe55:1b91, NextHop:0:0:0:0:0:0:0:0, mask: 128`	There is no functional impact. Port **`shutdown`** and **`no shutdown`** commands, which recovers the traffic, works even when the switch is in an error state.
VOSS-2285	When on BEB, continuously pinging IPv6 neighbor address using CLI command **`ping -s`**, ping packets do not drop, but instead return no answer messages.	Restart the ping. Avoid intensive CPU processing.
VOSS-2333	Layer 2 ping to Virtual BMAC (VBMAC) fails, if the VBMAC is reachable via Layer 2 core.	None.
VOSS-2397	If you configure a channelized port in EDM by using the **Configuration** > **Edit** > **Port** > **General** or **Configuration** > **Edit** >	In the Device Physical View, right-click the port and use the **General** > **IP** or

Table continues…

Issue number	Description	Workaround
	Port > **IP**or **IPv6** navigation paths, you can only see and configure the first sub-port.	**General** > **IPv6** sub-menu to configure all sub-ports.
VOSS-2411	On a VSP 4450GSX-DC, the https-port info is not displayed or saved into the configuration.	None.
VOSS-2415	There is no option in the Insert V3 Interface screen of EDM to insert a VRRPv3 interface for IPv6. The two check boxes in the screen are disabled.	There is no functional impact. EDM has two menus of IP and IPv6 and this functionality is available there along with other features.
VOSS-2418	When you configure and enable the SLA Mon agent, the SLA Mon server is able to discover it but the agent registration on the switch does not occur.	None.
VOSS-2422	When a BGP Neighbor times out, the following error message occurs: `CP1 [03/11/16 13:43:39.084:EST] 0x000b45f2 00000000 GlobalRouter SW ERROR ip_rtdeleteVrf: orec is NULL!`	There is no functional impact. Ignore the error message.
VOSS-2859	You cannot modify the port membership on a protocol-based VLAN using EDM, after it has been created.	Use CLI to provision the port membership on the protocol-based VLAN or delete the protocol-based VLAN, and then re-create it with the correct port member setting.
VOSS-3393	When the SLA Mon agent IP is created on a CLIP interface, the switch provides the CLIP-id as the agent MAC.	There is no functional impact. Use different CLIP IDs to differentiate the SLA Mon agents from the SLA Mon server.
VOSS-4255	If you run IP traceroute from one end host to another end host with a DvR Leaf in between, an intermediate hop will appear as not responding because the Leaf does not have an IP interface to respond. The IP traceroute to the end host will still work.	None.
VOSS-4728	If you remove and recreate an IS-IS instance on an NNI port with autonegotiation enabled in addition to vIST and R/SMLT enabled, it is possible that the NNI port will briefly become operationally down but does recover quickly. This operational change can lead to a brief traffic loss and possible reconvergence if non-ISIS protocols like OSPF or BGP are also on the NNI port.	If you need to remove and recreate an IS-IS instance on an autonegotiation enabled NNI port that also has non-ISIS traffic, do so during a maintenance window to minimize possible impact to other non-ISIS traffic.
VOSS-4840	If you run the **`show fulltech`** command in an SSH session, do not disable SSH on	None.

Table continues…

Issue number	Description	Workaround
	the system. Doing so can block the SSH session.	
VOSS-4912	The VSP 4000 Series does not advertise an LLDP Management TLV.	None.
VOSS-5130	Disabling and immediately enabling IS-IS results in the following log message: `PLSBFIB ERROR: /vob/cb/nd_protocols/plsb/lib/plsbFib.cpp(line 1558) unregisterLocalInfo() local entry does not exist. key(0xfda010000fffa40)`	There is no functional impact. Ignore the error message.
VOSS-5159 & VOSS-5160	If you use a CLIP address as the management IP address, the switch sends out 127.1.0.1 as the source IP address in both SMTP packets and TACACS+ packets.	None.
VOSS-5173	A device on a DvR VLAN cannot authenticate using RADIUS if the RADIUS server is on a DvR VLAN on a DvR Leaf using an in-band management IP address.	Place the RADIUS server in a non-DvR VLAN off a DvR Leaf or DvR Controller.
VOSS-5197	A BGP peer-group is uniquely identified by its name and not by its index. It is possible that the index that is configured for a peer-group changes between system reboots; however this has no functional impact.	None.
VOSS-5331	When you enable FHS ND inspection on a VLAN, and an IPv6 interface exists on the same VLAN, the IPv6 host client does not receive a ping response from the VLAN.	None.
VOSS-5603	In a scaled DvR environment (scaled DvR VLANs), you may see a higher CPU utilization while deleting a DvR leaf node from the DvR domain (no dvr leaf). The CPU utilization stays higher for several minutes on that node only and then returns to normal after deleting all the internal VLANs on the leaf node.	It is recommended to use a maintenance window when removing leaf(s) from a DvR domain.
VOSS-5627	The system does not currently restrict the number of VLANs on which you can simultaneously configure NLB and Directed Broadcast, resulting in resource hogging.	Ensure that you configure NLB and Directed Broadcast on not more that 100 VLANs simultaneously, assuming one NLB cluster for each VLAN. Also, ensure that you configure NLB on a VLAN first, and then Directed Broadcast, so as to not

Table continues…

Issue number	Description	Workaround
		exhaust the NLB and Directed Broadcast shared resources. The shared resources are NLB interfaces and VLANs with Directed Broadcast enabled. The permissible limit for the shared resources is 200.
VOSS-5982	When using Microsoft Edge to login to EDM, the first attempt fails if you use http.	Use https, another browser (Firefox or Internet Explorer), or login a second time.
VOSS-6189	When you connect to EDM using HTTPS in Microsoft Edge or Mozilla FireFox, the configured values for the RADIUS KeepAliveTimer and CFM SBM MepId do not appear.	Use Internet Explorer when using an HTTPS connection.
VOSS-6822	If the IPsec/IKE software used in the Radius server side is strongSwan, there is a compatibility issue between VOSS and strongSwan in terms of IPv6 Digicert (IKEv1/v2) authentication.	None.
VOSS-6928	On VSP 8000 Series platforms, IPv4 Filters with redirect next hop action do not forward when a default route is not present or a VLAN common to ingress VLAN of the filtered packet is not present.	Configure a default route if possible.
VOSS-7006	SMLT MACs are not synced correctly when you create a new VLAN on one of the vIST peers.	After you create a VLAN, enter the following command: **vlan mac-address-entry <vlan id> re-sync**
VOSS-7058	Redirect to the next-hop ACL takes longer than expected to become active after a link down/link up scenario.	Configure a dummy static route pointing to the next-hop.
VOSS-7139	DHCPv6 Snooping is not working in an SPB network as the DHCPv6 Snooping entries are not being displayed.	Administrator should add manual entries.
VOSS-7457	The switch can experience an intermittent traffic loss after you disable a Fabric Extend tunnel.	Bounce the tunnel between the devices.
VOSS-7471	EDM does not provide a menu for valid TCP flag options when configuring an ACL/ACE filter. You cannot see what flags are supported for eq and mask.	Use CLI, which shows the valid TCP flag options.
VOSS-7472	EDM shows incorrect guidance for ACL TCP flag mask. EDM reports `0…63` as hexadecimal. CLI correctly shows `<0-0x3F | 0-63> Mask value <Hex`	Use CLI to see the correct unit values.

Table continues…

Issue number	Description	Workaround
	`| Decimal>`. This is a display issue only with no functional impact.	
VOSS-7495	The VSP 4000 Series CLI Help text shows an incorrect port for **`boot config flags linerate-directed-broadcast`**. The Help text shows 1/48. The correct port is 1/46.	None
VOSS-7553	Option to configure the default queue profile rate-limit and weight values are inconsistent between EDM and CLI. Option to configure default values is missing in EDM.	None.
VOSS-8424	A fragmented ping from an external device to a switch when the VLAN IP interface is tied to a non-default VRF fails.	None.
VOSS-8516	Secure Copy (SCP) cannot use 2048-bit public DSA keys from Windows.	Use 1024/2048-bit RSA keys or 1024-bit DSA keys.
VOSS-9206	Interface statistics InDiscard counter in **`show interfaces gigabitEthernet error`** output does not increment consistently when IPv6 packets are dropped when uRPF checks fail. This issue applies only to VSP 4000 Series.	None.
VOSS-9516	When you connect to EDM using HTTPS, you can see multiple `SSL negotiation with client successful` messages during your EDM session. This message appears each time a successful SSL_Handshake occurs between the web browser and the web server. The log file may not show as many messages as the console and the timing between messages can be different because logging does not occur in real time.	None.
VOSS-9589	Dynamic Nickname Assignment is not supported over Fabric Extend tunnels.	None.
VOSS-9621	For VOSS products, 1G Copper Pluggable auto-negotiation is always enabled after a reboot, despite configuration settings.	If you do not want to use auto-negotation, disable it after the reboot.
VOSS-9642	If you add more ports to an existing MLT used by an IPv6 tunnel to send traffic, the datapath records do not update to support the new port.	Do not add ports to an MLT if an IPv6 tunnel terminates on an MLT. For example, when MLT is used as the tunnel next hop.

Table continues…

Issue number	Description	Workaround
		You can bounce the MLT links to re-trigger the tunnel information download.
VOSS-9670	When rebooting the chassis, the following message can appear: `1 2018-03-05T11:16:36.168-05:00 AVL-156 CP1 - 0x002bc608 - 00000000 GlobalRouter VSPTALK WARNING cppTap unexpected IO error fd 137 errno 100.`	None. VSP Talk is not a supported VOSS feature.
VOSS-9917	The log message `INFO Switch Externally Rebooted with CoreDump` does not consistently appear on the console port before reboot when you select the **softResetCoreDump** option from EDM.	None.
VOSS-9921	Bootup redirection timeout is longer than the UNI port (SMLT) unlock timer. If both vIST nodes boot together in factory default configuration fabric mode or without a nickname, the vIST ports will not enable for up to 4 minutes. During the delay the nickname server is unreachable and vIST is not online.	None.
VOSS-10380	If you enable and configure IPv6 Source Guard and EAPoL on a port, and create and configure a Guest VLAN on the same port without DHCP Snooping and ND-inspection, no error is shown. The port is not added to the Guest VLAN.	None.
VOSS-10381	If you enable and configure IPv6 Source Guard and EAPoL MHSA on a port, and create and configure RAVs for Non-EAP clients on the same port without DHCP Snooping and ND-inspection, no error is shown. The client displays as authenticated into RAV, even when port is not a member of RAV.	None.
VOSS-10412	Removal of the QSFP+ to SFP+ adapter with a 10G pluggable is not detected on the VSP 8404 and VSP 8404C when in non channelized mode.	The QSFP+ to SFP+ adapter and detection works only on ports with channelization enabled.
VOSS-10574	IS-IS sys-name output is not truncated for **`show isis spbm nick-name`** or **`show ip route`** commands. If a long character sys-name is in use, the full sys-name	None.

Table continues…

Issue number	Description	Workaround
	display can cause misalignment of the output columns.	
VOSS-10815	DvR over SMLT: Traffic is lost at failover on SMLT towards EXOS switches. DvR hosts are directly connected to the DvR controllers vIST pair on SMLT LAG and switched-UNIs are dynamically added using Fabric Attach. Only occurs when the access SMLT is LACP MLT and all the ports in the MLT are down. When all ports in the MLT down and an ARP request is received over an NNI link, there is no physical port that can be associated with the ARP request. The ARP entry is learned against NNI link, and MAC syncs from vIST peer or from a non-vIST peer when bouncing vIST.	None.
VOSS-10891	DvR leaf vIST: Wrong rarSmltCheckSmltPeerMac MLT warning displays when the peer vIST MAC address is learned from local	None. rarSmltCheckSmltPeerMac MLT warning has no functional impact. You can ignore the error message.
VOSS-11084	In highly scaled environments the command **`show vnid mac-address-entry`** can be slow in printing the expected output.	None.
VOSS-11196	IPFIX counts UNI-to-NNI and NNI-to-UNI flows twice.	None.
VOSS-11480	In a VXLAN Gateway configuration, the host MAC access learned against the VXLAN tunnel is deleted when no traffic passes through it for a short time. The MAC address is learned again when the traffic resumes or after the next mac-age timer when the vIST peer synchronizes with the peer.	None.
VOSS-11895	In a vIST SMLT environment where streams are both local and remote, if source and receiver port links are removed and reinserted several times, eventually traffic will not be forwarded to local single-homed receivers on one peer if the traffic is ingressing from the vIST peer over the NNI link. If the stream ingresses locally, it is received by the local UNI receivers.	Disable and renable Fabric Multicast (**`spbm <1-100> multicast enable`**) on the source VLAN to allow the streams to be deleted and come back in properly.

Table continues…

Issue number	Description	Workaround
VOSS-11943	This release does not support per-port configuration of Application Telemetry. Because the feature is enabled globally and VSP 7432CQ supports 32 100 Gbps ports, an undesirable condition may be encountered when an exceeded amount of Application Telemetry mirrored packets are sent to the collector.	None.
VOSS-12229	In a vIST/SMLT scenario with IGMP SPB snooping receivers on an SMLT link using IGMPv3, and the sender is local to one of the vIST peers, if you shut down the SMLT ports to change the MLT group membership or change the MLT type from SMLT admin to normal MLT, when you bring the ports back up, traffic from the stream may no longer flow to receivers on the SMLT link.	Use the following workarounds: 1. Shut down the lowest port number *last*, which avoids the issue. 2. If you do not shut down ports as specified in the preceding bullet, then after you change the MLT group membership of an SMLT MLT or change an administrative type SMLT to a normal MLT, bounce the multicast protocol on the SMLT VLANs so that receivers will be learned on the proper set of ports (**`no ip igmp snooping`** followed by **`ip igmp snooping`**).
VOSS-12330	When accesssing the on-switch RESTCONF API documentation in a web browser, the page does not render correctly.	Ensure you include the trailing slash (/) in the URL: `http(s)://<ip-address>:8080/apps/restconfdoc/`. For more information, see Configuring User Interfaces and Operating Systems for VOSS.
VOSS-12352	The response time for the RESTCONF get-operation gets slower proportional to the number of VLANs.	None.
VOSS-12390	Do not use the **`exit`** command from within the Extreme Insight analytics VM if you access the VM with the **`virtual-services console`** command; doing so makes the console non-responsive.	Disable and enable the VM or, alternatively, use an SSH connection.
VOSS-12405	To reach a VM, all front panel traffic must travel through an Insight port, which is a 10 Gbps port. If front panel port traffic is over 10 Gbps, this situation represents an oversubscription on the Insight port and some of the packets will be dropped. As a result, Extreme Management Center can lose connectivity to the Analytics engine if Application Telemetry is enabled.	None.

Restrictions and Expected Behaviors

This section lists known restrictions and expected behaviors that may first appear to be issues.

General Restrictions and Expected Behaviors

The following table provides a description of the restriction or behavior.

Issue number	Description	Workaround
—	If you access the Extreme Insight virtual machine using **`virtual-service tpvm console`** and use the Nano text editor inside the console access, the command **`^o<cr>`** does not write the file to disk.	None.
VOSS-7	Even when you change the LLDP mode of an interface from CDP to LLDP, if the remote side sends CDP packets, the switch accepts them and refreshes the existing CDP neighbor entry.	Disable LLDP on the interface first, and then disable CDP and re-enable LLDP.
VOSS-687	EDM and CLI show different local preference values for a BGP IPv6 route. EDM displays path attributes as received and stored in the BGP subsystem. If the attribute is from an eBGP peer, the local preference appears as zero. CLI displays path attributes associated with the route entry, which can be modified by a policy. If a route policy is not configured, the local preference shows the default value of 100.	None.
VOSS-1954	After you log in to EDM, if you try to refresh the page by clicking on the refresh button in the browser toolbar, it will redirect to a blank page. This issue happens only for the very first attempt and only in Firefox.	To refresh the page and avoid this issue, use the EDM refresh button instead of the browser refresh button. If you do encounter this issue, place your cursor in the address bar of the browser, and press **Enter**. This will return you to the EDM home page.
VOSS-2166	The IPsec security association (SA) configuration has a NULL Encryption option under the **Encrpt-algo** parameter. Currently, you must fill the **encrptKey** and **keyLength** sub-parameters to set this option; however,	There is no functional impact due to this configuration and it only leads to an unnecessary configuration step. No workaround required.

Table continues…

Issue number	Description	Workaround
	these values are not used for actual IPsec processing as it is a NULL encryption option. The NULL option is required to interoperate with other vendors whose IPsec solution only supports that mode for encryption.	
VOSS-2185	MAC move of the client to the new port does not automatically happen when you move a Non-EAP client authenticated on a specific port to another EAPoL or Non-EAP enabled port.	As a workaround, perform one of the following tasks: • Clear the non-EAP session on the port that the client is first authenticated on, before you move the client to another port. • Create a VLAN on the switch with the same VLAN ID as that dynamically assigned by the RADIUS server during client authentication. Use the command **`vlan create <2-4059> type port-mstprstp <0-63>`**. Ensure that the new port is a member of this VLAN.
VOSS-7640	The same route is learned via multiple IPv6 routing protocols (a combination of two of the following : RIPng, OSPFv3 and BGPv6). In this specific case, an eBGP (current best – preference 45) route is replaced by and iBGP (preference 175) which in turn is replaced by and OSPFv3 (external 2) route (preference 125).	None.
VOSS-7647	With peer group configuration, you cannot configure Update Source interface with IPv6 loopback address in EDM.	Use CLI.
VOSS-9174	OVSDB remote VTEP and MAC details can take between 5 to 10 minutes to populate and display after a HW-VTEP reboots.	Known issue in VMware NSX 6.2.4. You can upgrade to NSX 6.4 to resolve this issue.
VOSS-9462	OVSDB VNID I-SID MAC bindings are not populated on HW-VTEPs after configuration changes.	Known issue in VMware NSX 6.2.4. You can upgrade to NSX 6.4 to resolve this issue.
VOSS-10168	The system CLI does not prevent you from using the same IP address for theVXLAN Gateway hardware VTEP	Manually check the IP configured as the OOB Management IP. Do not use the OOB Management IP address as the replication remote peer IP address.

Table continues…

Issue number	Description	Workaround
	replication remote peer IP and OOB Management IP.	
VOSS-11817	The OVS connect-type for virtual service Vports is designed in such a way that it connects to any generic virtual machine (VM) guest OS version using readily available Ethernet device drivers. This design approach provides initial connectivity to the VM in a consistent manner. A consequence of this approach is that Vports created with connect-type OVS will show up as 1 Gbps interfaces in the VM even though the underlying Ethernet connection supports 10 Gbps .	If additional performance is desired, upgrade the VM guest OS with an Ethernet device driver that supports 10 Gbps interfaces.
VOSS-12151	If logical switch has only hardware ports binding, and not VM behind software VTEP, Broadcast, Unknown Unicast, and Multicast (BUM) traffic does not flow between host behind two hardware VTEP. The NSX replicator node handles the BUM traffic. NSX does not create the replicator node unless a VM is present. In an OVSDB topology, it is expected that at least one VM connects to the software VTEP. This issue is an NSX-imposed limitation.	After you connect the VM to the software VTEP, the issue is not seen.
VOSS-12395	You cannot use the following cables on 10 Gb fiber interfaces, or 40 Gb channelized interfaces, with the QSA28 adapter: • 1, 3, and 5 meter QSFP28 25 Gb DAC • 20 meter QSFP28 25 Gb AOC	n/a
wi01068569	The system displays a warning message that routes will not inject until the apply command is issued after the enable command. The warning applies only after you enable redistribution, and not after you disable redistribution. For example: **`Switch:1(config)#isis apply redistribute direct vrf 2`**	n/a

Table continues…

Issue number	Description	Workaround
wi01112491	IS-IS enabled ports cannot be added to an MLT. The current release does not support this configuration.	n/a
wi01122478	Stale SNMP server community entries for different VRFs appear after reboot with no VRFs. On a node with a valid configuration file saved with more than the default vrf0, SNMP community entries for that VRF are created and maintained in a separate text file, `snmp_comm.txt`, on every boot. The node reads this file and updates the SNMP communities available on the node. As a result, if you boot a configuration that has no VRFs, you may still see SNMP community entries for VRFs other than the globalRouter vrf0 .	n/a
wi01137195	A static multicast group cannot be configured on a Layer 2 VLAN before enabling IGMP snooping on the VLAN. After IGMP snooping is enabled on the Layer 2 VLAN for the first time, static multicast group configuration is allowed, even when IGMP snooping is disabled later on that Layer 2 VLAN.	n/a
wi01138851	Configuring licenses using EDM is not supported.	n/a
wi01141638	When a VLAN with 1000 multicast senders is deleted, the console or Telnet session stops responding and SNMP requests time out for up to 2 minutes.	n/a
wi01142142	When a multicast sender moves from one port to another within the same BEB or from one vIST peer BEB to another, with the old port operationally up, the source port information in the output of the **`show ip igmp sender`** command is not updated with new sender port information.	You can perform one of the following workarounds: • On an IGMP snoop-enabled interface, you can flush IGMP sender records. **Caution:** Flushing sender records can cause a transient traffic loss. • On an IGMP-enabled Layer 3 interface, you can toggle the IGMP state.

Table continues…

Issue number	Description	Workaround
		Caution: Expect traffic loss until IGMP records are built after toggling the IGMP state.
wi01145099	IP multicast packets with a time-to-live (TTL) equal to 1 are not switched across the SPB cloud over a Layer 2 VSN. They are dropped by the ingress BEB.	To prevent IP multicast packets from being dropped, configure multicast senders to send traffic with TTL greater than 1.
wi01159075	VSP 4450GTX-HT-PWR+: Mirroring functionality is not working for RSTP BPDUs.	None.
wi01171670	Telnet packets get encrypted on MACsec enabled ports.	None.
wi01198872	On VSP 4000 Series, a loss of learned MAC addresses occurs in a vIST setup beyond 10k addresses. In a SPB setup the MAC learning is limited to 13k MAC addresses, due to the limitation of the internal architecture when using SPB. Moreover, as vIST uses SPB and due to the way vIST synchronizes MAC addresses with a vIST pair, the MAC learning in a vIST setup is limited to 10K Mac addresses.	None.
wi01210217	The command **`show eapol auth-stats`** displays `LAST-SRC-MAC` for NEAP sessions incorrectly.	n/a
wi01211415	In addition to the fan modules, each power supply also has a fan. The power supply stops working if a power supply fan fails, but there is no LED or software warning that indicates this failure.	Try to recover the power supply fan by resetting the switch. If the fan does not recover, then replace the faulty power supply.
wi01212034	When you disable EAPoL globally: • Traffic is allowed for static MAC configured on EAPoL enabled port without authentication. • Static MAC config added for authenticated NEAP client is lost.	n/a
wi01212247	BGP tends to have many routes. Frequent additions or deletions impact network connectivity. To prevent	Bounce the BGP protocol globally.

Table continues…

Issue number	Description	Workaround
	frequent additions or deletions, reflected routes are not withdrawn from client 2 even though they are withdrawn from client 1. Disabling route-reflection can create a black hole in the network.	
wi01212585	LED blinking in EDM is representative of, but not identical to, the actual LED blinking rates on the switch.	n/a
wi01213040	When you disable auto-negotiation on both sides, the 10 Gbps copper link does not come up.	n/a
wi01213066 wi01213374	EAP and NEAP are not supported on brouter ports.	n/a
wi01213336	When you configure tx mode port mirroring on T-UNI and SPBM NNI ports, unknown unicast, broadcast and multicast traffic packets that ingress these ports appear on the mirror destination port, although they do not egress the mirror source port. This is because tx mode port mirroring happens on the mirror source port before the source port squelching logic drops the packets at the egress port.	n/a
wi01219658	The command **`show khi port-statistics`** does not display the count for NNI ingress control packets going to the CP.	n/a
wi01219295	SPBM QOS: Egress UNI port does not follow port QOS with ingress NNI port and Mac-in-Mac incoming packets.	n/a
wi01223526	ISIS logs duplicate system ID only when the device is a direct neighbor.	n/a
wi01223557	Multicast outage occurs on LACP MLT when simplified vIST peer is rebooted.	You can perform one of the following work arounds: • Enable PIM on the edge. • Ensure that IST peers are either RP or DR but not both.
wi01224683 wi01224689	Additional link bounce may occur on 10 Gbps ports when toggling links or during cable re-insertion.	n/a

Table continues…

Issue number	Description	Workaround
	Additional link bounce may occur with 40 Gbps optical cables and 40 Gbps break-out cables, when toggling links or during cable re-insertion.	
wi01229417	Origination and termination of IPv6 6-in-4 tunnel is not supported on a node with vIST enabled.	None.
wi01232578	When SSH keyboard-interactive-auth mode is enabled, the server generates the password prompt to be displayed and sends it to the SSH client. The server always sends an expanded format of the IPv6 address. When SSH keyboard-interactive-auth mode is disabled and password-auth is enabled, the client itself generates the password prompt, and it displays the IPv6 address format used in the **`ssh`** command.	None.
wi01234289	HTTP management of the ONA is not supported when it is deployed with a VSP 4000 Series device.	None.

VSP 4450GTX-HT-PWR+ Restrictions

⚠ Caution:

The VSP 4450GTX-HT-PWR+ has operating temperature and power restrictions. For safety and optimal operation of the device, ensure that the prescribed thresholds are strictly adhered to.

The following table provides a description of the restriction or behavior and the work around, if one exists.

Behavior	Description	Workaround
For high-temperature threshold	The VSP 4450GTX-HT-PWR+ supports a temperature range of 0°C to 70°C. In the alpha release, power supply does not shut down at an intended over-temperature threshold of 79°C.	To prevent equipment damage, ensure that the operating temperature is within the supported temperature range of 0°C to 70°C.
For power supply wattage threshold	Software functionality to reduce the POE power budget based on the number of operational power supplies and operating temperature is not available in the Alpha SW image.	Ensure that the POE device power draw is maintained at the following when the device is at temperatures between 61°C and 70°C: • 400W — with 1 operational power supply

Table continues…

Behavior	Description	Workaround
		• 832W — with 2 operational power supplies
For inoperable external USB receptacle	The VSP 4450GTX-HT-PWR+ has an empty external USB receptacle that was not available in GTS models. Software to support the use of the external USB receptacle is not yet available in the Alpha SW image. Therefore the USB port is inoperable.	No workarounds are provided with the alpha image.

SSH Connections

VOSS 4.1.0.0 and VOSS 4.2.0.0 SSH server and SSH client support password authentication mode.

VOSS 4.2.1.0 changed the SSH server from password authentication to keyboard-interactive. VOSS 4.2.1.0 changed the SSH client to automatically support either password authentication or keyboard-interactive mode.

In VOSS 4.2.1.0, you cannot configure the SSH server to support password authentication. This limitation creates a backward compatibility issue for SSH clients that do not support keyboard-interactive mode, including SSH clients that are part of pre-VOSS 4.2.1.0 software releases. For example, VOSS 4.1.0.0 SSH clients, VOSS 4.2.0.0 SSH clients, and external SSH clients that only support password authentication cannot connect to VOSS 4.2.1.0 SSH servers.

This issue is addressed in software release VOSS 4.2.1.1 and later. The default mode of the SSH server starting from VOSS 4.2.1.1 is changed back to password authentication. Beginning with VOSS 5.0, you can use a CLI command to change the SSH server mode to keyboard-interactive.

For more information about how to configure the SSH server authentication mode, see Administering VOSS.

See the following table to understand SSH connections between specific client and server software releases.

Client software release	Server software release	Support
VOSS 4.1.0.0	VOSS 4.2.0.0	Supported
VOSS 4.1.0.0	VOSS 4.2.1.0	Not supported
VOSS 4.2.0.0	VOSS 4.2.1.0	Not supported
VOSS 4.1.0.0	VOSS 4.2.1.1	Supported
VOSS 4.2.0.0	VOSS 4.2.1.1	Supported

Fabric Extend IP over ELAN/VPLS

This feature allows multiple switches running Fabric Extend IP to be directly connected over a Layer 2 broadcast domain without the need for loopback VRFs in Release 6.0 or later.

Releases earlier than 6.0 have a single next hop/ARP restriction that require the use of loopback VRFs to deploy Fabric Extend IP over ELAN/VPLS.

For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.

Redirect Next-hop Filter Restrictions

This feature does not behave the same way on all platforms:

- VSP 4000 Series and VSP 7400 Series

  The redirect next-hop filter redirects packets with a time-to-live (TTL) of 1 rather than sending them to the CPU where the CPU would generate ICMP TTL expired messages. IP Traceroute does not correctly report the hop. For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.

- VSP 7200 Series and VSP 8000 Series

  The redirect next-hop filter does not redirect packets with a time-to-live (TTL) of 1 nor does it send them to the CPU where the CPU would generate ICMP TTL expired messages. IP Traceroute reports a timeout for the hop. For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.

IP Source Guard Restrictions

If you enable Application Telemetry, IPv6 Source Guard commands and configurations are blocked and not available on VSP 4000 Series, VSP 7200 Series, and VSP 8000 Series switches.

Filter Restrictions

The following table identifies known restrictions.

Applies To	Restriction
All platforms	The switch does not support logging and PCAP with filters.
ACL restrictions	
All platforms	Only port-based ACLs are supported on egress. VLAN-based ACLs are not supported.
All platforms	IPv6 ingress and egress QoS ACL/filters are not supported.
All platforms	Control packet action is not supported on InVSN Filter or IPv6 filters generally.
All platforms	IPv4/IPv6 VLAN based ACL filters will be applied on traffic received on all the ports if it matches VLAN ID associated with the ACL.
VSP 7200 Series VSP 7400 Series VSP 8000 Series	VLAN ID and VLAN_DOT1p attributes for untagged traffic are not supported for ingress/egress filters.
All platforms	Scaling numbers are reduced for IPv6 filters.
All platforms	The InVSN Filter does supports IP Shortcut traffic only on both UNI and NNI ports, but does not support IP Shortcut traffic on UNI ports only and NNI ports only.
All platforms	The InVSN Filter does not filter packets that arrive on NNI ingress ports but are bridged to other NNI ports or are for transit traffic.
All platforms	You can insert an inVsn ACL type for a Switched UNI only if the Switched UNI I-SID is associated with a platform VLAN.

Table continues…

Applies To	Restriction
ACE restrictions	
All platforms	When an ACE with action count is disabled, the statistics associated with the ACE are reset.
All platforms	Only security ACEs are supported on egress. QoS ACEs are not supported.
All platforms	ICMP type code qualifier is supported only on ingress filters.
All platforms	For port-based ACLs, you can configure VLAN qualifiers. Configuring port qualifiers are not permitted.
All platforms	For VLAN-based ACLs, you can configure port qualifiers. Configuring VLAN qualifiers are not permitted.
All platforms	Egress QoS filters are not supported for IPv6 filters.
All platforms	Ingress QoS filters are not supported for IPv6 filters.
All platforms	Source/Destination MAC addresses cannot be added as attributes for IPv6 filters ACEs.
VSP 4000 Series VSP 7200 Series VSP 8000 Series	If more than 256 IPv6 filters are configured, the number of IPv4 filters is reduced.
VSP 4000 Series VSP 7200 Series VSP 8000 Series	If you enable Application Telemetry, IPv6 security filter commands and configurations are blocked and not available.

Chapter 8: Resolved Issues

This section details the issues that are resolved in this release.

Fixes from Previous Releases

VOSS 8.0 incorporates all fixes from prior releases, up to and including VOSS 6.1.6.0 and 7.1.1.0.

Resolved Issues in VOSS 8.0

Issue number	Description
VOSS-7443	You may detect MHMV ports in the NULL VLAN.
VOSS-7528	If user changes spbm ethertype to 0x88A8 instead of the default value of 0x8100, B-VLAN TPID remains still 0x8100 over FE tunnels.
VOSS-9943	The system displays the unnecessary error message `Error: FHS supported only on IPv6 interfaces associated with GlobalRouter.` when you clear FHS statistics using the **`clear ipv6 fhs statistics all`** command without an FHS configuration.
VOSS-10716	Ping failure from device to destination in directly attached networks when VRF is different than the source VRF. Occurs only when the source and destination are in different VRFs, and the destination is in a directly attached network, and the packet originated from CP or is destined to CP.
VOSS-10730	When ISIS accept policy is applied either directly or indirectly, direct routes redistribute from one VRF to another. The presense of the same route in the data structures causes an IP error. For example, IP errors are seen after applying **`isis accept policy`** or **`isis adjacency flap`**.
VOSS-10842	DvR Failover: When powering down a controller, the remaining controller does not advertise domain hosts in the backbone. Hosts are seen from other controllers in the backbone but cannot import correctly.
VOSS-10913	Missing interface gigabitEthernet from running config when only mac-security limit-learning is enabled on port.
VOSS-11070	Removed unsupported fonts and replaced with supported ones to improve page response/load times.
VOSS-11072	If you run the **`ip igmp flush vlan <vlanid> sender <a.b.c.d> <w.x.y.x>`** or the corresponding SNMP set to flush an IGMP sender entry, the operation fails with `Error: Operation not allowed without a proper license file installed.`
VOSS-11083	DHCP configuration fails to load on reboot when MSDP enabled in VRF.

Table continues…

Issue number	Description
VOSS-11335	Fixed a high CPU issue in **`show ip igmp snoop-trace`** command when **`show fulltech`** is issued.
VOSS-11644	VOSS 7.0 does not log message when incorrect power supply DPS-800RB Q is installed.
VOSS-11693	Enhanced warning message when Resource Manager allocations are used up.
VOSS-11834	VOSS 7.x does not allow VLAN list to be added to ACL when configured from CLI.
VOSS-11855 VOSS-11917	Nonexistent adjacency advertised in IS-IS TLV22's adjacency list. The issue occurs when: • more than 13 adjacencies exist. Only 13 adjacencies can fit inside the 255-bytes limit of an individual TLV. When more than 13 adjacencies exist, multiple TLV22s are allocated to hold all adjacencies. • the I1-metric of one of the IS-IS interfaces is modified, or a new IS-IS interface is created with a non-default I1-metric. • an IS-IS adjacency bounces or goes down and stays down.
VOSS-11996	All VLACP interfaces timed out on the box due to buffer exhaustion.
VOSS-12045	Fixed an erroneous message when **`backup configure`** command is executed.
VOSS-12212 VSP8000-355	If you use a 40 Gbps Direct Attach Cable (DAC) between VSP 8400 Series and ExtremeSwitching X690, the link is not established.
VSP4000-231	Clean-up of ACL entries after administratively shut MLT port is removed.
VSP4000-235	SNMPv3 informs in authPriv mode do not work with Extreme Management Center server.
VSP4000-236	Memory leak when SLAMon is configured
VSP4000-239	Discarding Gratuitous ARP packet having opcode GRAT ARP REPLY.
VSP4000-242	Unable to Communicate between VRF interfaces.
VSP7200-62 VOSS-10742	**`show interfaces gigabitEhernet i-sid`** command caused an out-of-bounds access issue.
VSP7200-68	EDM not showing optic module info TX Power (Actual Value) and duplicates Fields in **Graph** > **Ethernet Errors** tab.
VSP7200-71	Device may reset when TACACS EDM user is configured with access level 15 and **`show fulltech`** or **`show user`** commands are run.
VSP8000-268	Connection via EDM failed for HTTP and HTTPS.
VSP8000-310	System reset triggered by VRRP thread pre-emption issue with fast advertisement interval configured.
VSP8000-315	Some VSP 8404 GS ESM ports are inaccessible after power glitch.
VSP8000-329	All VLACP interfaces timed out on the box due to buffer exhaustion.

Table continues…

Issue number	Description
VSP8000-330 VSP8000-336	EDM connectivity issues due to memory leak.
VSP8000-338	System stability issues when accessing the device through SSH.
VSP8000-340	Problem with hot plugging 40G modules into 8418XTQ ESM in VSP 8404C.
VSP8000-348	VSP 8404 - Unable to upgrade from 6.1.4 to 7.0 with no cards in the chassis.
VSP8000-351	Enhanced log message to display CLI port numbers instead of BCM port numbers.
VSP8000-358 VOSS-11826	Device may reset while adding MSDP Peer. Configuring MSDP on SPBM-enabled devices that are linked by eBGP and have a BGP route causes a device reset.
VSP8000-362	ISIS:LSP TLV22 contains stale adjacency info after l1-metric change.
VSP8000-366	40G Optics information not seen on VSP 8400 Hardware revision 2 running on 7.1 software version.

Appendix A: Related Information

Features by Release

The following table identifies the release that first introduced feature support on a hardware platform. Each new release includes all the features from previous releases unless specifically stated otherwise.

Note:

Release 4.1 was the first VOSS release. Release numbers earlier than 4.1 are releases specific to the particular platform.

Table 25: Features by Release

Feature	Product	Release introduced
Access Control List (ACL)-based filtering, including egress ACLs, ingress ACLs, Layer 2 to Layer 4 filtering, port-based, and VLAN-based For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Address Resolution Protocol (ARP) including Proxy ARP and Static ARP For more information, see Configuring IPv4 Routing for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series Series	4.2
Advanced Feature Bandwidth Reservation For more information, see Administering VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	n/a
	VSP 7400 Series	8.0 VSP 7432CQ reserves 2 ports (low): 1/31 and 1/32
	VSP 8200 Series	n/a

Table continues…

Feature	Product	Release introduced
	VSP 8400 Series	n/a
Alternative routes for IPv4 For more information, see Configuring IPv4 Routing for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Alternative routes for IPv6 For more information, see Configuring IPv6 Routing for VOSS.	VSP 4450 Series	5.1
	VSP 7200 Series	5.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1
	VSP 8400 Series	5.1
Application Telemetry For more information, see Monitoring Performance for VOSS.	VSP 4450 Series	7.1
	VSP 7200 Series	7.1
	VSP 7400 Series	8.0
	VSP 8200 Series	7.1
	VSP 8400 Series	7.1
Automatic QoS For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Backup configuration and restore For more information, see Administering VOSS.	VSP 4450 Series	6.1.2
	VSP 7200 Series	6.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1.2
	VSP 8400 Series	6.1.2
Border Gateway Protocol for IPv4 (BGPv4) For more information, see Configuring BGP Services for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
BGP+ (BGPv4 for IPv6). For more information, see Configuring BGP Services for VOSS.	VSP 4450 Series	5.0
	VSP 7200 Series	5.0
	VSP 7400 Series	8.0

Table continues…

Feature	Product	Release introduced
	VSP 8200 Series	5.0
	VSP 8400 Series	5.0
BGPv6 For more information, see Configuring BGP Services for VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	8.0
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
Bridge Protocol Data Unit (BPDU) Guard For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS.	VSP 4450 Series	6.0
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
CFM configuration on C-VLANs For more information, see Troubleshooting VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	n/a
	VSP 7400 Series	n/a
	VSP 8200 Series	n/a
	VSP 8400 Series	n/a
Certificate order priority **Note:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.1.2
	VSP 7200 Series	5.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1.2
	VSP 8400 Series	5.1.2
Channelization of 40 Gbps ports For more information, see the hardware documentation and Administering VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.2
	VSP 8400 Series	4.2
Channelization of 100 Gbps ports For more information, see the hardware documentation and Administering VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	n/a
	VSP 7400 Series	8.0
	VSP 8200 Series	n/a
	VSP 8400 Series	n/a
Command Line Interface (CLI) For more information, see Configuring User Interfaces and Operating Systems for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1

Table continues…

Feature	Product	Release introduced
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
DHCPv6 Guard For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.0
	VSP 7200 Series	5.0
	VSP 7400 Series	8.0
	VSP 8200 Series	5.0
	VSP 8400 Series	5.0
DHCP Snooping(IPv4) For more information, see Configuring Security for VOSS.	VSP 4450 Series	6.1
	VSP 7200 Series	6.1
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1
	VSP 8400 Series	6.1
DHCP Snooping (IPv6) For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.1
	VSP 7200 Series	5.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1
	VSP 8400 Series	5.1
Digital Certificate/PKI **Note:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.1.2
	VSP 7200 Series	5.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1.2
	VSP 8400 Series	5.1.2
Differentiated Services (DiffServ) including Per-Hop Behavior For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Directed Broadcast For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.1.1
	VSP 7200 Series	5.1.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1.1
	VSP 8400 Series	5.1.1
Distributed Virtual Routing (DvR) controller	VSP 4450 Series	n/a

Table continues…

Feature	Product	Release introduced
For more information, see Configuring IPv4 Routing for VOSS. **Important:** Because of a change in 6.0.1.2, we recommend a *minimum* software version of 6.0.1.2 in DvR deployments.	VSP 7200 Series	6.0.1
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0.1
	VSP 8400 Series	6.0.1
Distributed Virtual Routing (DvR) leaf For more information, see Configuring IPv4 Routing for VOSS. **Important:** Because of a change in 6.0.1.2, Extreme Networks recommends a *minimum* software version of 6.0.1.2 in DvR deployments.	VSP 4450 Series	6.1
	VSP 7200 Series	6.0.1
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0.1
	VSP 8400 Series	6.0.1
Domain Name Service (DNS) client (IPv4) For more information, see Administering VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Dot1Q MIB • dot1VlanCurrentTable • dot1qVlanStaticTable • dot1qPortVlanTable • dot1dBasePortEntry • dot1qVlanNumDelete	VSP 4450 Series	6.1.2
	VSP 7200 Series	6.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1.2
	VSP 8400 Series	6.1.2
DNS client (IPv6) For more information, see Administering VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
Dynamic ARP Inspection (DAI) For more information, see Configuring Security for VOSS.	VSP 4450 Series	6.1
	VSP 7200 Series	6.1
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1
	VSP 8400 Series	6.1
Dynamic Host Configuration Protocol (DHCP) Relay, DHCP Option 82 For more information, see Configuring IPv4 Routing for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0

Table continues…

Feature	Product	Release introduced
	VSP 8400 Series	4.2
Dynamic Nickname Assignment For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	N/A
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
Egress port mirror For more information, see Troubleshooting VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	n/a
	VSP 7400 Series	n/a
	VSP 8200 Series	n/a
	VSP 8400 Series	n/a
Egress port shaper For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Encryption modules The encryption modules file is included in the runtime software image file; it is not a separate file.	VSP 4450 Series	4.2
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.2
	VSP 8400 Series	4.2
Energy Saver For more information, see Administering VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0 VSP 7254XTQ only
	VSP 7400 Series	n/a
	VSP 8200 Series	n/a
	VSP 8400 Series	7.0
Enhanced Secure mode For more information, see Administering VOSS.	VSP 4450 Series	4.2
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.2
	VSP 8400 Series	4.2
Enhanced Secure mode for JITC and non-JITC sub-modes. For more information, see Administering VOSS.	VSP 4450 Series	5.1
	VSP 7200 Series	5.1

Table continues…

Feature	Product	Release introduced
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1
	VSP 8400 Series	5.1
Enterprise Device Manager (EDM) For more information, see Configuring User Interfaces and Operating Systems for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
EDM representation of physical LED status For more information, see the hardware documentation for your platform.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.2
	VSP 8400 Series	4.2
Entity MIB - Physical Table For more information, see Administering VOSS.	VSP 4450 Series	6.0
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
Entity MIB enhancements and integration for the following: • Physical Table • Alias Mapping Table • Physical Contains Table • Last Change Time object For more information, see Administering VOSS.	VSP 4450 Series	6.1.2
	VSP 7200 Series	6.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1.2
	VSP 8400 Series	6.1.2
Equal Cost Multiple Path (ECMP) for IPv4 For more information, see Configuring IPv4 Routing for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
ECMP for IPv6 For more information, see the following documents: • Configuring IPv4 Routing for VOSS • Configuring BGP Services for VOSS • Configuring IPv6 Routing for VOSS	VSP 4450 Series	5.1
	VSP 7200 Series	5.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1
	VSP 8400 Series	5.1
ECMP support for VXLAN Gateway and Fabric Extend	VSP 4450 Series	n/a

Table continues…

Feature	Product	Release introduced
For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS.	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
Equal Cost Trees (ECT) For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
E-Tree and Private VLANs For more information about E-Tree, see Configuring Fabric Basics and Layer 2 Services for VOSS . For more information about Private VLANs, see Configuring VLANs, Spanning Tree, and NLB for VOSS . For information about how to configure MLT and Private VLANs, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
Extensible Authentication Protocol (EAP) and EAP over LAN (EAPoL) For more information, see Configuring Security for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
EAPoL MHMA-MV For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.1
	VSP 7200 Series	5.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1
	VSP 8400 Series	5.1
EAPoL enhancements: Enhanced MHMV, Fail Open VLAN, Guest VLAN For more information, see Configuring Security for VOSS.	VSP 4450 Series	6.1
	VSP 7200 Series	6.1
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1
	VSP 8400 Series	6.1
External BGP (EBGP) For more information, see Configuring BGP Services for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0

Table continues…

Feature	Product	Release introduced
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
Extreme Insight For more information, see Configuring User Interfaces and Operating Systems for VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	n/a
	VSP 7400 Series	8.0
	VSP 8200 Series	n/a
	VSP 8400 Series	n/a
Extreme Management Center backup configuration ZIP file For more information, see Extreme Management Center documentation.	VSP 4450 Series	6.1.2
	VSP 7200 Series	6.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1.2
	VSP 8400 Series	6.1.2
Fabric Attach For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 4450 Series	5.0
	VSP 7200 Series	5.0
	VSP 7400 Series	8.0
	VSP 8200 Series	5.0
	VSP 8400 Series	5.0
Fabric Attach Zero Touch Client Attachment For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 4450 Series	6.0
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
Fabric BCB mode For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Fabric BEB mode For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Fabric Connect services with switch cluster	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1

Table continues…

Feature	Product	Release introduced
For more information, see the Fabric Connect documents: • Configuring Fabric Basics and Layer 2 Services for VOSS • Configuring Fabric Layer 3 Services for VOSS • Configuring Fabric Multicast Services for VOSS	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Fabric Extend For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS. *Platforms require an Open Networking Adapter (ONA).	VSP 4450 Series	5.0*
	VSP 7200 Series	5.0
	VSP 7400 Series	8.0
	VSP 8200 Series	5.0
	VSP 8400 Series	5.0
Fabric RSPAN (Mirror to I-SID) For more information, see Troubleshooting VOSS.	VSP 4450 Series	6.0 Flow-based mirroring into single I-SID only
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
FDB protected by port (MAC security limit-learning) For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	n/a
	VSP 7400 Series	n/a
	VSP 8200 Series	n/a
	VSP 8400 Series	n/a
File Transfer Protocol (FTP) server and client (IPv4) For more information, see Administering VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
File Transfer Protocol (FTP) server and client (IPv6) For more information, see Administering VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
FHS - DHCPv6 Guard For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.0
	VSP 7200 Series	5.0
	VSP 7400 Series	8.0

Table continues…

Feature	Product	Release introduced
	VSP 8200 Series	5.0
	VSP 8400 Series	5.0
FHS - DHCP Snooping (IPv4) For more information, see Configuring Security for VOSS.	VSP 4450 Series	6.1
	VSP 7200 Series	6.1
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1
	VSP 8400 Series	6.1
FHS - DHCP Snooping (IPv6) For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.1
	VSP 7200 Series	5.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1
	VSP 8400 Series	5.1
FHS - IP Source Guard (IPv4 and IPv6) For more information, see Configuring Security for VOSS.	VSP 4450 Series	6.1
	VSP 7200 Series	6.1
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1
	VSP 8400 Series	6.1
FHS - Neighbor Discovery Inspection (IPv6) For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.1
	VSP 7200 Series	5.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1
	VSP 8400 Series	5.1
FHS - IPv6 Router Advertisement (RA) Guard For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.0
	VSP 7200 Series	5.0
	VSP 7400 Series	8.0
	VSP 8200 Series	5.0
	VSP 8400 Series	5.0
Flight Recorder for system health monitoring For more information, see Troubleshooting VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Forward Error Correction (FEC) (configurable) For more information, see Administering VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	n/a

Table continues…

Feature	Product	Release introduced
	VSP 7400 Series	8.0
	VSP 8200 Series	n/a
	VSP 8400 Series	8.0
Gratuitous ARP filtering For more information, see Configuring IPv4 Routing for VOSS.	VSP 4450 Series	4.2
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.2
	VSP 8400 Series	4.2
High Availability-CPU (HA-CPU) For more information, see Administering VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	n/a
	VSP 7400 Series	n/a
	VSP 8200 Series	n/a
	VSP 8400 Series	n/a
IEEE 802.1ag Connectivity Fault Management (CFM): • Layer 2 Ping • TraceRoute • TraceTree For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
IEEE 802.3X Pause frame transmit For more information, see Administering VOSS.	VSP 4450 Series	6.0
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
Industry Standard Discovery Protocol (ISDP) (CDP compatible) For more information, see Administering VOSS.	VSP 4450 Series	6.0
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
Ingress dual rate port policers For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	n/a
	VSP 7400 Series	n/a
	VSP 8200 Series	n/a
	VSP 8400 Series	n/a
Internal BPG (IBGP)	VSP 4450 Series	4.2

Table continues…

Feature	Product	Release introduced
For more information, see Configuring BGP Services for VOSS.	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.2
	VSP 8400 Series	4.2
Internet Control Message Protocol (ICMP) For more information, see Configuring IPv4 Routing for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
ICMP broadcast and multicast enable or disable For more information, see Configuring IPv4 Routing for VOSS and Configuring IPv6 Routing for VOSS.	VSP 4450 Series	5.1
	VSP 7200 Series	5.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1
	VSP 8400 Series	5.1
Internet Group Management Protocol (IGMP), including virtualization For more information, see Configuring IP Multicast Routing Protocols for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0.1
	VSP 8400 Series	4.2
Internet Key Exchange (IKE) v2 **Note:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.1.2
	VSP 7200 Series	5.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1.2
	VSP 8400 Series	5.1.2
Internet Protocol Flow Information eXport (IPFIX) For more information, see Monitoring Performance for VOSS	VSP 4450 Series	n/a
	VSP 7200 Series	n/a
	VSP 7400 Series	8.0
	VSP 8200 Series	n/a
	VSP 8400 Series	n/a
Inter-VSN routing (IPv4) For more information, see Configuring Fabric Layer 3 Services for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2

Table continues…

Feature	Product	Release introduced
Inter-VSN routing (IPv6) For more information, see Configuring Fabric Layer 3 Services for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
InVSN Filter For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	8.0
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
IP Multicast over Fabric Connect For more information, see Configuring Fabric Multicast Services for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
IP route policies For more information, see Configuring IPv4 Routing for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
IP Shortcut routing including ECMP For more information, see Configuring Fabric Layer 3 Services for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
IP Source Guard (IPv4 and IPv6) For more information, see Configuring Security for VOSS.	VSP 4450 Series	6.1
	VSP 7200 Series	6.1
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1
	VSP 8400 Series	6.1
IP Source Routing enable or disable For more information, see Configuring IPv4 Routing for VOSS and Configuring IPv6 Routing for VOSS.	VSP 4450 Series	5.1
	VSP 7200 Series	5.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1

Table continues…

Feature	Product	Release introduced
	VSP 8400 Series	5.1
IPsec for the Out-of-band management port (IPv4) For more information, see Configuring Security for VOSS.	VSP 4450 Series	4.2
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0VSP 8200 Series
	4.2	
	VSP 8400 Series	4.2
IPsec for the Out-of-band management port (IPv6) For more information, see Configuring Security for VOSS.	VSP 4450 Series	6.0
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
IPv6 (OSPFv3, VRRP, RSMLT, DHCP Relay, IPv4 in IPv6 tunnels) For more information, see Configuring IPv6 Routing for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
IPv6 ACL filters For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
IPv6 egress filters For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	8.0
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
IPv6 mode flag (**`boot config flags ipv6-mode`**) For more information, see Configuring IPv6 Routing for VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
IPv6 Router Advertisement (RA) Guard For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.0
	VSP 7200 Series	5.0
	VSP 7400 Series	8.0

Table continues…

Feature	Product	Release introduced
	VSP 8200 Series	5.0
	VSP 8400 Series	5.0
IPv6 Shortcut routing For more information, see Configuring Fabric Layer 3 Services for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
IPv6 Virtualization for the following features and functions: • IPv6 Interfaces and IPv6 Static Routes in VRFs and Layer 3 VSNs • ECMP and Alternative route • Route redistribution for static and direct routes • VRRPv3 for IPv6 • DHCP Relay • IPv6 Reverse Path Forwarding • ICMP Ping and Traceroute For more information, see Configuring IPv6 Routing for VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	8.0
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
IPv6 Virtualization for the following features and functions: • Open Shortest Path First for IPv6 (OSPFv3) • IPv6 Border Gateway Protocol (IPv6 BGP) • IPv6 route redistribution enhancements For more information, see Configuring IPv6 Routing for VOSS.	VSP 4450 Series	8.0
	VSP 7200 Series	8.0
	VSP 7400 Series	8.0
	VSP 8200 Series	8.0
	VSP 8400 Series	8.0
IPv4 IS-IS accept policies For more information, see Configuring Fabric Layer 3 Services for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
IPv6 IS-IS accept policies For more information, see Configuring Fabric Layer 3 Services for VOSS.	VSP 4450 Series	8.0
	VSP 7200 Series	8.0
	VSP 7400 Series	8.0
	VSP 8200 Series	8.0
	VSP 8400 Series	8.0
IS-IS authentication with SHA-256	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	8.0

Table continues…

Feature	Product	Release introduced
For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
Key Health Indicator (KHI) For more information, see Monitoring Performance for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Layer 2 Video Surveillance install script For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 4450 Series	6.1
	VSP 7200 Series	6.1
	VSP 7400 Series	n/a
	VSP 8200 Series	6.1
	VSP 8400 Series	6.1
Layer 2 Virtual Service Network (VSN) For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Layer 3 switch cluster (Routed SMLT) with Simplified vIST For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0.1
	VSP 8400 Series	4.2
Layer 3 switch cluster (Routed SMLT) with Virtual Inter-Switch Trunk (vIST) For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Layer 3 Video Surveillance install script (formerly known as the run vms endura script) For more information, see Configuring Fabric Layer 3 Services for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	n/a
	VSP 7400 Series	n/a
	VSP 8200 Series	n/a
	VSP 8400 Series	n/a
Layer 3 VSN	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1

Table continues…

Feature	Product	Release introduced
For more information, see Configuring Fabric Layer 3 Services for VOSS.	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
License files signed using Extreme Networks signature.	VSP 4450 Series	6.1.2
	VSP 7200 Series	6.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1.2
	VSP 8400 Series	6.1.2
linerate-directed-broadcast boot flag (**`boot config flags linerate-directed-broadcast`**) For more information, see Administering VOSS.	VSP 4450 Series	6.1
	VSP 7200 Series	n/a
	VSP 7400 Series	n/a
	VSP 8200 Series	n/a
	VSP 8400 Series	n/a
Link Layer Discovery Protocol (LLDP) For more information, see Administering VOSS.	VSP 4450 Series	6.0
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
LLDP-MED For more information, see Administering VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	n/a
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
Link-state tracking (LST) For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	n/a
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
Linux kernel version **Important:** For VSP 4450 Series, VSP 7200 Series, VSP 8200, and VSP 8400 Series, kernel version 4.9 has special upgrade considerations the *first* time you upgrade to a release that supports it. You must first upgrade to a stepping-stone	VSP 4450 Series	4.9 as of VOSS 7.0
	VSP 7200 Series	4.9 as of VOSS 7.0
	VSP 7400 Series	4.14 as of VOSS 8.0
	VSP 8200 Series	4.9 as of VOSS 7.0
	VSP 8400 Series	4.9 as of VOSS 7.0

Table continues…

Feature	Product	Release introduced
release, 6.1.x , *before* you upgrade to the release with the new kernel.		
Logging to a file and syslog (IPv4) For more information, see Monitoring Performance for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Logging to a file and syslog (IPv6) For more information, see Monitoring Performance for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
Logon banner **Note:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see Administering VOSS.	VSP 4450 Series	5.1.2
	VSP 7200 Series	5.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1.2
	VSP 8400 Series	5.1.2
MACsec 2AN mode **Note:** VOSS 5.0 officially removes the replay protection commands. Do not use replay protection in earlier releases. For more information, see Configuring Security for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	n/a
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
MACsec 4AN mode For more information, see Configuring Security for VOSS.	VSP 4450 Series	6.0
	VSP 7200 Series	6.0
	VSP 7400 Series	n/a
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
Mirroring (port and flow-based) For more information, see Troubleshooting VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
MSTP-Fabric Connect Multi Homing	VSP 4450 Series	7.0

Table continues…

Feature	Product	Release introduced
For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 7200 Series	7.0
	VSP 7400 Series	8.0
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
Multicast Listener Discovery (MLD) For more information, see Configuring IP Multicast Routing Protocols for VOSS.	VSP 4450 Series	5.1
	VSP 7200 Series	5.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1
	VSP 8400 Series	5.1
Multicast route (mroute) statistics for IPv4 and IPv6 For more information, see Configuring IP Multicast Routing Protocols for VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	5.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1
	VSP 8400 Series	5.1
MultiLink Trunking (MLT) / Link Aggregation Group (LAG) For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Multiple CLI users per role For more information, see Administering VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	8.0
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
Multiple IS-IS parallel adjacencies For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	8.0
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
Neighbor Discovery Inspection (IPv6) For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.1
	VSP 7200 Series	5.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1
	VSP 8400 Series	5.1

Table continues…

Feature	Product	Release introduced
Network Load Balancing (NLB) - multicast operation For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
Network Load Balancing (NLB) - unicast operation For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
NTPv3 client For more information, see Administering VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
NTPv3 with SHA authentication For more information, see Administering VOSS.	VSP 4450 Series	5.1
	VSP 7200 Series	5.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1
	VSP 8400 Series	5.1
NTPv4 client for IPv4 For more information, see Administering VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	8.0
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
NTPv4 client for IPv6 For more information, see Administering VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	8.0
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
NTPv4 master and restrict	VSP 4450 Series	8.0
	VSP 7200 Series	8.0
	VSP 7400 Series	8.0
	VSP 8200 Series	8.0

Table continues…

Feature	Product	Release introduced
	VSP 8400 Series	8.0
nni-mstp boot flag (**`boot config flags nni-mstp`**) **Important:** This flag has special upgrade considerations the first time you upgrade to a release that supports it. For more information, see Administering VOSS.	VSP 4450 Series	6.0
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
Non EAPoL MAC RADIUS authentication For more information, see Configuring Security for VOSS.	VSP 4450 Series	4.2.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.2.1
	VSP 8400 Series	4.2.1
Open Shortest Path First (OSPF) For more information, see Configuring OSPF and RIP for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
OVSDB protocol support for VXLAN Gateway For more information, see Configuring VXLAN Gateway for VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	7.1
	VSP 7400 Series	8.0
	VSP 8200 Series	7.1
	VSP 8400 Series	7.1
P-Bridge MIB Adds support for: • dot1dExtBase Group • dot1dDeviceCapabilities • dot1dTrafficClassesEnabled • dot1dGmrpStatus • dot1dPortCapabilitiesTable	VSP 4450 Series	6.1.2
	VSP 7200 Series	6.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1.2
	VSP 8400 Series	6.1.2
Protocol Independent Multicast-Sparse Mode (PIM-SM), PIM-Source Specific Mode (PIM-SSM) for IPv4 For more information, see Configuring IP Multicast Routing Protocols for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0.1
	VSP 8400 Series	4.2
PIM over IPv6	VSP 4450 Series	5.1
	VSP 7200 Series	5.1

Table continues…

Feature	Product	Release introduced
For more information, see Configuring IP Multicast Routing Protocols for VOSS.	VSP 7400 Series	8.0
	VSP 8200 Series	5.1
	VSP 8400 Series	5.1
Power Management For more information, see Administering VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	n/a
	VSP 7400 Series	n/a
	VSP 8200 Series	n/a
	VSP 8400 Series	n/a
Power over Ethernet (PoE) For more information, see Administering VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	n/a
	VSP 7400 Series	n/a
	VSP 8200 Series	n/a
	VSP 8400 Series	n/a
PoE/PoE+ allocation using LLDP For more information, see Administering VOSS.	VSP 4450 Series	5.1
	VSP 7200 Series	n/a
	VSP 7400 Series	n/a
	VSP 8200 Series	n/a
	VSP 8400 Series	n/a
QoS Access Control Entries (ACE) For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
QoS ingress port rate limiter For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	4.2.1
	VSP 7400 Series	n/a
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
QoS per queue rate limiting For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	VSP 4450 Series	5.1
	VSP 7200 Series	5.1.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1.1
	VSP 8400 Series	5.1.1
QoS Priority Assignment	VSP 4450 Series	7.0

Table continues…

Feature	Product	Release introduced
For more information, see Configuring Security for VOSS.	VSP 7200 Series	7.0
	VSP 7400 Series	8.0
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
RADIUS (IPv6) For more information, see Configuring Security for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
RADIUS attributes: • Acct-Terminate-Cause • Event-Timestamp • Service Type For more information, see Configuring Security for VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	8.0
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
RADIUS, community-based users (IPv4) For more information, see Configuring Security for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
RADIUS secure communication using IPSec for IPv4 **Note:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.1.2
	VSP 7200 Series	5.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1.2
	VSP 8400 Series	5.1.2
RADIUS secure communication using IPSec for IPv6 **Note:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.1.2
	VSP 7200 Series	5.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1.2
	VSP 8400 Series	5.1.2
Read-Only user for EDM For more information, see Configuring User Interfaces and Operating Systems for VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	8.0
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0

Table continues…

Feature	Product	Release introduced
Remote Login (Rlogin) server/client (IPv4) For more information, see Administering VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Rlogin server (IPv6) For more information, see Administering VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
Remote Monitoring 1 (RMON1) for Layer 1 and Layer 2 **Note:** Release 5.0 and 5.1 do not support RMON1. For more information, see Monitoring Performance for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Remote Monitoring 2 (RMON2) for network and application layer protocols For more information, see Monitoring Performance for VOSS.	VSP 4450 Series	4.2
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.2
	VSP 8400 Series	4.2
Remote Shell (RSH) server/client For more information, see Administering VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
RFC 5176 – Dynamic Authorization Extensions to RADIUS For more information, see Configuring Security for VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	8.0
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
RFC 5997 – RADIUS Reachability Server Status For more information, see Configuring Security for VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	8.0
	VSP 8200 Series	7.0

Table continues…

Feature	Product	Release introduced
	VSP 8400 Series	7.0
Representational State Transfer Configuration Protocol (RESTCONF) For more information, see Configuring User Interfaces and Operating Systems for VOSS.	VSP 4450 Series	8.0
	VSP 7200 Series	8.0
	VSP 7400 Series	8.0
	VSP 8200 Series	8.0
	VSP 8400 Series	8.0
Route Information Protocol (RIP) For more information, see Configuring OSPF and RIP for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Route metric for BGP route redistribution For more information, see Configuring BGP Services for VOSS.	VSP 4450 Series	6.1
	VSP 7200 Series	6.1
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1
	VSP 8400 Series	6.1
RIPng For more information, see Configuring IPv6 Routing for VOSS.	VSP 4450 Series	5.0
	VSP 7200 Series	5.0
	VSP 7400 Series	8.0
	VSP 8200 Series	5.0
	VSP 8400 Series	5.0
run spbm installation script For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
Russia summer time zone change For more information, see Administering VOSS.	VSP 4450 Series	4.2
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.2
	VSP 8400 Series	4.2
Secure Copy (SCP) **Note:** The switch does not support the WinSCP client.	VSP 4450 Series	4.0
	VSP 7200 Series	5.0
	VSP 7400 Series	8.0

Table continues…

Feature	Product	Release introduced
For more information, see Administering VOSS.	VSP 8200 Series	4.0
	VSP 8400 Series	5.0
Secure hash algorithm 1 (SHA-1) and SHA-2 For more information, see Configuring OSPF and RIP for VOSS.	VSP 4450 Series	4.2
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.2
	VSP 8400 Series	4.2
Secure Shell (SSH) (IPv4) For more information, see Administering VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Secure Sockets Layer (SSL) certificate management For more information, see Administering VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
Security ACEs For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Segmented Management Instance For more information, see Administering VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	8.0
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0
Segmented Management Instance — ability to migrate VLAN or loopback IP address For more information, see Administering VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	n/a
	VSP 7400 Series	n/a
	VSP 8200 Series	n/a
	VSP 8400 Series	n/a
sFlow For more information, see Monitoring Performance for VOSS.	VSP 4450 Series	6.0
	VSP 7200 Series	6.0

Table continues…

Feature	Product	Release introduced
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
sFlow collector reachability on user-created VRFs For more information, see Monitoring Performance for VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	n/a
	VSP 7400 Series	8.0
	VSP 8200 Series	n/a
	VSP 8400 Series	n/a
Simple Loop Prevention Protocol (SLPP) For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Simple Mail Transfer Protocol (SMTP) for log notification For more information, see Monitoring Performance for VOSS.	VSP 4450 Series	6.0
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
Simple Network Management Protocol (SNMP) v1/2/3 (IPv4) For more information, see Configuring Security for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
SLA Mon For more information, see Configuring the SLA Mon Agent for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
SLPP Guard For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.	VSP 4450 Series	6.1
	VSP 7200 Series	6.1
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1
	VSP 8400 Series	6.1
SNMP (IPv6)	VSP 4450 Series	4.1

Table continues…

Feature	Product	Release introduced
For more information, see Configuring Security for VOSS.	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
SONMP For more information, see Administering VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Spanning Tree Protocol (STP): • Multiple STP (MSTP) • Rapid STP (RSTP) For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
spbm-config-mode (**`boot config flags spbm-config-mode`**) For more information, see Configuring IP Multicast Routing Protocols for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0.1
	VSP 8400 Series	4.2
SPB-PIM Gateway controller node For more information see Configuring Fabric Multicast Services for VOSS.	VSP 4450 Series	6.0
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
SPB-PIM Gateway interface For more information see Configuring Fabric Multicast Services for VOSS.	VSP 4450 Series	6.0
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
SSH (IPv6) For more information, see Administering VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2

Table continues…

Feature	Product	Release introduced
SSH client disable For more information, see Administering VOSS.	VSP 4450 Series	6.0
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
SSH key sizes in multiples of 1024 **Note:** Releases 6.0 and 6.0.1 do not support this change. For more information, see Administering VOSS.	VSP 4450 Series	5.1.2
	VSP 7200 Series	5.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1.2
	VSP 8400 Series	5.1.2
SSH rekey For more information, see Administering VOSS.	VSP 4450 Series	5.1
	VSP 7200 Series	5.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1
	VSP 8400 Series	5.1
Static routing For more information, see Configuring IPv4 Routing for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Suspend duplicate system ID detection For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 4450 Series	6.1
	VSP 7200 Series	6.1
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1
	VSP 8400 Series	6.1
Switch cluster (multi-chassis LAG) -Virtual Inter-Switch Trunk (vIST) For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Switched UNI For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 4450 Series	5.0
	VSP 7200 Series	5.0
	VSP 7400 Series	8.0
	VSP 8200 Series	5.0

Table continues…

Feature	Product	Release introduced
	VSP 8400 Series	5.0
System Logging compliance with RFC 5424 and RFC 3339	VSP 4450 Series	6.1.2
	VSP 7200 Series	6.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	6.1.2
	VSP 8400 Series	6.1.2
TACACS+ For more information, see Configuring Security for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
TACACS+ secure communication using IPSec for IPv4 **Note:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.1.2
	VSP 7200 Series	5.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1.2
	VSP 8400 Series	5.1.2
Telnet server and client (IPv4) For more information, see Administering VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Telnet server and client (IPv6) For more information, see Administering VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
TCP timestamp control For more information, see Configuring Security for VOSS.	VSP 4450 Series	8.0
	VSP 7200 Series	8.0
	VSP 7400 Series	8.0
	VSP 8200 Series	8.0
	VSP 8400 Series	8.0
TLS server for secure HTTPS **Note:** Releases 6.0 and 6.0.1 do not support this feature.	VSP 4450 Series	5.1.2
	VSP 7200 Series	5.1.2
	VSP 7400 Series	8.0

Table continues…

Feature	Product	Release introduced
For more information, see Configuring User Interfaces and Operating Systems for VOSS.	VSP 8200 Series	5.1.2
	VSP 8400 Series	5.1.2
TLS client for secure syslog **Note:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see Troubleshooting VOSS. lease	VSP 4450 Series	5.1.2
	VSP 7200 Series	5.1.2
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1.2
	VSP 8400 Series	5.1.2
Transparent Port UNI (T-UNI) For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.2.1
	VSP 8400 Series	4.2.1
Trivial File Transfer Protocol (TFTP) server and client (IPv4) For more information, see Administering VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
TFTP server and client (IPv6) For more information, see Administering VOSS.	VSP 4450 Series	4.1
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.1
	VSP 8400 Series	4.2
Two Factor Authentication for SSH For more information, see Configuring Security for VOSS.	VSP 4450 Series	8.0
	VSP 7200 Series	8.0
	VSP 7400 Series	8.0
	VSP 8200 Series	8.0
	VSP 8400 Series	8.0
Unicast Reverse Path Forwarding (URPF) checking (IPv4 and IPv6) For more information, see Configuring Security for VOSS.	VSP 4450 Series	5.0
	VSP 7200 Series	5.0
	VSP 7400 Series	8.0
	VSP 8200 Series	5.0
	VSP 8400 Series	5.0
Virtual Link Aggregation Control Protocol (VLACP)	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1

Table continues…

Feature	Product	Release introduced
For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Virtual Router Redundancy Protocol (VRRP) For more information, see Configuring IPv4 Routing for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Virtualization with IPv4 Virtual Routing and Forwarding (VRF) • ARP • DHCP Relay • Inter-VRF Routing (static, dynamic, and policy) • Local routing • OSPFv2 • RIPv1 and v2 • Route policies • Static routing • VRRP For more information, see Configuring IPv4 Routing for VOSS.	VSP 4450 Series	4.0
	VSP 7200 Series	4.2.1
	VSP 7400 Series	8.0
	VSP 8200 Series	4.0
	VSP 8400 Series	4.2
Increased VRF and Layer 3 VSN scaling For more information, see Configuring IPv4 Routing for VOSS.	VSP 4450 Series	6.0
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0
VRRPv3 for IPv4 and IPv6 For more information, see Configuring IPv4 Routing for VOSS and Configuring IPv6 Routing for VOSS.	VSP 4450 Series	5.1
	VSP 7200 Series	5.1
	VSP 7400 Series	8.0
	VSP 8200 Series	5.1
	VSP 8400 Series	5.1
VXLAN Gateway For more information, see Configuring VXLAN Gateway for VOSS.	VSP 4450 Series	n/a
	VSP 7200 Series	6.0
	VSP 7400 Series	8.0
	VSP 8200 Series	6.0
	VSP 8400 Series	6.0

Table continues…

Feature	Product	Release introduced
Zero Touch Fabric configuration For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	VSP 4450 Series	7.0
	VSP 7200 Series	7.0
	VSP 7400 Series	N/A
	VSP 8200 Series	7.0
	VSP 8400 Series	7.0

MIB Changes

Deprecated MIBs

Table 26: Common

Object Name	Object OID	Deprecated in VOSS Release
rcChasFanTable	1.3.6.1.4.1.2272.1.4.7.1	7.0
rcChasFanEntry	1.3.6.1.4.1.2272.1.4.7.1.1	7.0
rcChasFanId	1.3.6.1.4.1.2272.1.4.7.1.1.1	7.0
rcChasFanOperStatus	1.3.6.1.4.1.2272.1.4.7.1.1.2	7.0
rcChasFanAmbientTemperature	1.3.6.1.4.1.2272.1.4.7.1.1.3	7.0
rcChasFanType	1.3.6.1.4.1.2272.1.4.7.1.1.4	7.0
rcChasLedTable	1.3.6.1.4.1.2272.1.4.65.1	7.0
rcChasLedEntry	1.3.6.1.4.1.2272.1.4.65.1.1	7.0
rcChasLedId	1.3.6.1.4.1.2272.1.4.65.1.1.1	7.0
rcChasLedLabel	1.3.6.1.4.1.2272.1.4.65.1.1.2	7.0
rcChasLedStatus	1.3.6.1.4.1.2272.1.4.65.1.1.3	7.0

Modified MIBs

Table 27: Common

Object Name	Object OID	Modified in VOSS Release	Modification
linkUp	1.3.6.1.6.3.1.1.5.3	7.1	To allow user or Extreme Management Center to display a port ifName instead of ifIndex, object ifName have been appended to 4th field in the trap Packet.
linkUp	1.3.6.1.6.3.1.1.5.4	7.1	To allow user or Extreme Management Center to display a port ifName instead of ifIndex, object ifName have been appended to 4th field in the trap Packet.
rcPrFilterAclMatchType	1.3.6.1.4.1.1.2272.1.202.1.1.2.3.1.1.19	7.1	ENUMERATE: Added Enum: uniOnly (1), both(3)
rcVossSystemTemperatureSensorIndex	1.3.6.1.4.1.2272.1.101.1.1.2.1.1	8.0	Changed the range from 1..4 to 1..7
rcVossSystemFanTrayInfoTrayId	1.3.6.1.4.1.2272.1.101.1.1.3.1.1	8.0	Changed the range from 1..5 to 1..6
rcVossSystemFanInfoTrayId	1.3.6.1.4.1.2272.1.101.1.1.4.1.1	8.0	Changed the range from 1..5 to 1..6
rcVossSystemCardLedId	1.3.6.1.4.1.2272.1.101.1.1.5.1.2	8.0	Changed the range from 1..4 to 1..5
rcCliUserPassword	1.3.6.1.4.1.2272.1.19.50.1.3	8.0	Changed the range from 0..256 to 0..80
rcPrFilterAceEthVlanIdVlanId	1.3.6.1.4.1.2272.1.202.1.1.2.4.7.1.7	8.0	Changed the range from 1..4084 to 1..4059
rcVrfRpTrigger	1.3.6.1.4.1.2272.1.203.1.1.1.2.1.9	8.0	definition of VrfRpTriggerBitCode changed to include ospfv3(8) as protocol
rcFanTrayId	1.3.6.1.4.1.2272.1.204.1.0.5	8.0	Changed the range from 1..2 to 1..6
rcLicenseLicenseType	1.3.6.1.4.1.2272.1.56.4	8.0	ADD_ENUM: Added enumeration "insight(14)"

Table continues…

Object Name	Object OID	Modified in VOSS Release	Modification
rcIsisPlsbIpv6UnicastFibEntry	1.3.6.1.4.1.2272.1.63.23.1	8.0	Added rcIsisPlsbIpInterIsidUnicastFibMetricType

Table 28: VSP 7400 Series

Object Name	Object OID	Modified in VOSS Release	Modification
rcVossSystemTemperatureSensorIndex	1.3.6.1.4.1.2272.1.101.1.1.2.1.1	8.0	Changed the range from 1..4 to 1..7
rcVossSystemCardLedId	1.3.6.1.4.1.2272.1.101.1.1.5.1.2	8.0	Changed the range from 1..4 to 1..5

New MIBs

Table 29: Common

Object Name	Object OID	New in VOSS Release
rcAppTelemetry	1.3.6.1.4.1.2272.1.226	7.1
rcAppTelemetryMib	1.3.6.1.4.1.2272.1.226.1	7.1
rcAppTelemetryNotifications	1.3.6.1.4.1.2272.1.226.1.1	7.1
rcAppTelemetryObjects	1.3.6.1.4.1.2272.1.226.1.2	7.1
rcAppTelemetryScalars	1.3.6.1.4.1.2272.1.226.1.2.1	7.1
rcAppTelemetryAdminEnable	1.3.6.1.4.1.2272.1.226.1.2.1.1	7.1
rcAppTelemetryClearCounterStats	1.3.6.1.4.1.2272.1.226.1.2.1.2	7.1
rcAppTelemetryCounterTable	1.3.6.1.4.1.2272.1.226.1.2.2	7.1
rcAppTelemetryCounterEntry	1.3.6.1.4.1.2272.1.226.1.2.2.1	7.1
rcAppTelemetryCounterId	1.3.6.1.4.1.2272.1.226.1.2.2.1.1	7.1
rcAppTelemetryCounterName	1.3.6.1.4.1.2272.1.226.1.2.2.1.2	7.1
rcAppTelemetryCounterPkts	1.3.6.1.4.1.2272.1.226.1.2.2.1.3	7.1
rcAppTelemetryCounterBytes	1.3.6.1.4.1.2272.1.226.1.2.2.1.4	7.1

Table continues…

Object Name	Object OID	New in VOSS Release
rcAppTelemetryCounterClearCounter	1.3.6.1.4.1.2272.1.226.1.2.2.1.5	7.1
rcNtpRestrictTable	1.3.6.1.4.1.2272.1.33.5	8.0
rcNtpRestrictEntry	1.3.6.1.4.1.2272.1.33.5.1	8.0
rcNtpRestrictRowIndex	1.3.6.1.4.1.2272.1.33.5.1.1	8.0
rcNtpRestrictAddressType	1.3.6.1.4.1.2272.1.33.5.1.2	8.0
rcNtpRestrictAddress	1.3.6.1.4.1.2272.1.33.5.1.3	8.0
rcNtpRestrictMask	1.3.6.1.4.1.2272.1.33.5.1.4	8.0
rcNtpRestrictRowStatus	1.3.6.1.4.1.2272.1.33.5.1.5	8.0
rcLicenseRemainingDays	1.3.6.1.4.1.2272.1.56.12	8.0
rcVossSystemMgmtPortLedStatus	1.3.6.1.4.1.2272.1.101.1.1.1.1	8.0
rcVossSystemControl	1.3.6.1.4.1.2272.1.101.1.1.1.2	8.0
rcVossSystemControlTcpTimestampEnable	1.3.6.1.4.1.2272.1.101.1.1.1.2.1	8.0
rcnRestConfServerOperationStatusTrap	1.3.6.1.4.1.2272.1.21.0.352	8.0
rcnChasPowerSupplyOppositeAirflowDetectedTrap	1.3.6.1.4.1.2272.1.21.0.353	8.0
rcnChasPowerSupplyOppositeAirflowClearTrap	1.3.6.1.4.1.2272.1.21.0.354	8.0
rcSflowExtRcvrTable	1.3.6.1.4.1.2272.1.221.1.1.3	8.0
rcSflowExtRcvrEntry	1.3.6.1.4.1.2272.1.221.1.1.3.1	8.0
rcSflowExtRcvrIsReachable	1.3.6.1.4.1.2272.1.221.1.1.3.1.2	8.0
rcSflowExtRcvrNextHop	1.3.6.1.4.1.2272.1.221.1.1.3.1.3	8.0
rcAppTelemetryRcvrIsReachable	1.3.6.1.4.1.2272.1.226.1.2.1.3	8.0
rcAppTelemetryRcvrNextHop	1.3.6.1.4.1.2272.1.226.1.2.1.4	8.0
rcRestConf	1.3.6.1.4.1.2272.1.227	8.0
rcRestConfObjects	1.3.6.1.4.1.2272.1.227.1	8.0
rcRestConfScalars	1.3.6.1.4.1.2272.1.227.1.1	8.0
rcRestConfGlobalEnable	1.3.6.1.4.1.2272.1.227.1.1.1	8.0
rcRestConfRestConfServerVersion	1.3.6.1.4.1.2272.1.227.1.1.10	8.0
rcRestConfTcpPort	1.3.6.1.4.1.2272.1.227.1.1.2	8.0
rcRestConfTlsEnable	1.3.6.1.4.1.2272.1.227.1.1.3	8.0

Table continues…

Object Name	Object OID	New in VOSS Release
rcRestConfCertificateFilename	1.3.6.1.4.1.2272.1.227.1.1.4	8.0
rcRestConfCertificateAction	1.3.6.1.4.1.2272.1.227.1.1.5	8.0
rcRestConfNotificationEnable	1.3.6.1.4.1.2272.1.227.1.1.6	8.0
rcRestConfOperStatus	1.3.6.1.4.1.2272.1.227.1.1.7	8.0
rcRestConfAddress	1.3.6.1.4.1.2272.1.227.1.1.8	8.0
rcRestConfWebServerVersion	1.3.6.1.4.1.2272.1.227.1.1.9	8.0
rcRestConfNotificationObjects	1.3.6.1.4.1.2272.1.227.1.2	8.0
rcRestConfServerOperationStatus	1.3.6.1.4.1.2272.1.227.1.2.1	8.0

Table 30: VSP 4000 Series

Object Name	Object OID	New in VOSS Release
rc2kPowerConsumptionInfoTable	1.3.6.1.4.1.2272.1.100.17	7.1

Table 31: VSP 7200 Series

Object Name	Object OID	New in VOSS Release
rcPortForwardErrorCorrection	1.3.6.1.4.1.2272.1.4.10.1.1.125	8.0
rcPortForwardErrorCorrectionApplicability	1.3.6.1.4.1.2272.1.4.10.1.1.126	8.0

Table 32: VSP 7400 Series

Object Name	Object OID	New in VOSS Release
rcPortForwardErrorCorrection	1.3.6.1.4.1.2272.1.4.10.1.1.125	8.0
rcPortForwardErrorCorrectionApplicability	1.3.6.1.4.1.2272.1.4.10.1.1.126	8.0
rcVirtualServiceVPortsTable	1.3.6.1.4.1.2272.1.101.1.1.10	8.0
rcVirtualServiceVPortsEntry	1.3.6.1.4.1.2272.1.101.1.1.10.1	8.0
rcVirtualServiceVPortsVirtServName	1.3.6.1.4.1.2272.1.101.1.1.10.1.1	8.0
rcVirtualServiceVPortsName	1.3.6.1.4.1.2272.1.101.1.1.10.1.2	8.0
rcVirtualServiceVPortsVlanIdList	1.3.6.1.4.1.2272.1.101.1.1.10.1.3	8.0

Table continues…

Object Name	Object OID	New in VOSS Release
rcVirtualServiceVPortsConnectType	1.3.6.1.4.1.2272.1.101.1.1.10.1.4	8.0
rcVirtualServiceVPortsRowStatus	1.3.6.1.4.1.2272.1.101.1.1.10.1.5	8.0
rcVirtualServiceApplicationTable	1.3.6.1.4.1.2272.1.101.1.1.11	8.0
rcVirtualServiceApplicationEntry	1.3.6.1.4.1.2272.1.101.1.1.11.1	8.0
rcVirtualServiceApplicationName	1.3.6.1.4.1.2272.1.101.1.1.11.1.1	8.0
rcVirtualServiceApplicationPackageName	1.3.6.1.4.1.2272.1.101.1.1.11.1.2	8.0
rcVirtualServiceApplicationReset	1.3.6.1.4.1.2272.1.101.1.1.11.1.3	8.0
rcVirtualServiceApplicationActionResult	1.3.6.1.4.1.2272.1.101.1.1.11.1.4	8.0
rcVirtualServiceApplicationInstallResult	1.3.6.1.4.1.2272.1.101.1.1.11.1.5	8.0
rcVirtualServiceApplicationRowStatus	1.3.6.1.4.1.2272.1.101.1.1.11.1.6	8.0
rcVirtualServiceScalars	1.3.6.1.4.1.2272.1.101.1.1.12	8.0
rcVirtualServiceHypervisorDiskRemain	1.3.6.1.4.1.2272.1.101.1.1.12.1	8.0
rcVirtualServiceHypervisorNumCoresRemain	1.3.6.1.4.1.2272.1.101.1.1.12.2	8.0
rcVirtualServiceHypervisorMemSizeRemain	1.3.6.1.4.1.2272.1.101.1.1.12.3	8.0
rcVossSystemInsightPackageFileTable	1.3.6.1.4.1.2272.1.101.1.1.13	8.0
rcVossSystemInsightPackageFileEntry	1.3.6.1.4.1.2272.1.101.1.1.13.1	8.0
rcVossSystemInsightPackageFileName	1.3.6.1.4.1.2272.1.101.1.1.13.1.1	8.0
rcVossSystemInsightPackageFileDate	1.3.6.1.4.1.2272.1.101.1.1.13.1.2	8.0
rcVossSystemInsightPackageFileSize	1.3.6.1.4.1.2272.1.101.1.1.13.1.3	8.0
rcVirtualServiceTable	1.3.6.1.4.1.2272.1.101.1.1.8	8.0
rcVirtualServiceEntry	1.3.6.1.4.1.2272.1.101.1.1.8.1	8.0

Table continues…

Object Name	Object OID	New in VOSS Release
rcVirtualServiceName	1.3.6.1.4.1.2272.1.101.1.1.8.1.1	8.0
rcVirtualServiceUtilCpuUtil	1.3.6.1.4.1.2272.1.101.1.1.8.1.10	8.0
rcVirtualServiceUtilMemAllot	1.3.6.1.4.1.2272.1.101.1.1.8.1.11	8.0
rcVirtualServiceUtilMemUsed	1.3.6.1.4.1.2272.1.101.1.1.8.1.12	8.0
rcVirtualServiceUtilMemAvailable	1.3.6.1.4.1.2272.1.101.1.1.8.1.13	8.0
rcVirtualServiceState	1.3.6.1.4.1.2272.1.101.1.1.8.1.14	8.0
rcVirtualServiceUpTime	1.3.6.1.4.1.2272.1.101.1.1.8.1.15	8.0
rcVirtualServiceRowStatus	1.3.6.1.4.1.2272.1.101.1.1.8.1.16	8.0
rcVirtualServiceHypervisorDiskRemain	1.3.6.1.4.1.2272.1.101.1.1.8.1.17	8.0
rcVirtualServiceHypervisorMemSizeRemain	1.3.6.1.4.1.2272.1.101.1.1.8.1.19	8.0
rcVirtualServiceNumCores	1.3.6.1.4.1.2272.1.101.1.1.8.1.2	8.0
rcVirtualServiceMemSize	1.3.6.1.4.1.2272.1.101.1.1.8.1.3	8.0
rcVirtualServiceEnable	1.3.6.1.4.1.2272.1.101.1.1.8.1.4	8.0
rcVirtualServicePackageInfoName	1.3.6.1.4.1.2272.1.101.1.1.8.1.5	8.0
rcVirtualServicePackageInfoPath	1.3.6.1.4.1.2272.1.101.1.1.8.1.6	8.0
rcVirtualServicePackageAppName	1.3.6.1.4.1.2272.1.101.1.1.8.1.7	8.0
rcVirtualServicePackageAppVersion	1.3.6.1.4.1.2272.1.101.1.1.8.1.8	8.0
rcVirtualServiceUtilCpuAllot	1.3.6.1.4.1.2272.1.101.1.1.8.1.9	8.0
rcVirtualServiceDiskTable	1.3.6.1.4.1.2272.1.101.1.1.9	8.0
rcVirtualServiceDiskEntry	1.3.6.1.4.1.2272.1.101.1.1.9.1	8.0

Table continues…

Object Name	Object OID	New in VOSS Release
rcVirtualServiceDiskVirtServName	1.3.6.1.4.1.2272.1.101.1.1.9.1.1	8.0
rcVirtualServiceDiskName	1.3.6.1.4.1.2272.1.101.1.1.9.1.2	8.0
rcVirtualServiceDiskSize	1.3.6.1.4.1.2272.1.101.1.1.9.1.3	8.0
rcVirtualServiceDiskSizeAllot	1.3.6.1.4.1.2272.1.101.1.1.9.1.4	8.0
rcVirtualServiceDiskSizeAvailable	1.3.6.1.4.1.2272.1.101.1.1.9.1.5	8.0
rcVirtualServiceDiskSizeUsed	1.3.6.1.4.1.2272.1.101.1.1.9.1.6	8.0
rcVirtualServiceDisksRowStatus	1.3.6.1.4.1.2272.1.101.1.1.9.1.7	8.0
rcPortForwardErrorCorrection	1.3.6.1.4.1.2272.1.4.10.1.1.125	8.0
rcPortForwardErrorCorrectionApplicability	1.3.6.1.4.1.2272.1.4.10.1.1.126	8.0
rcIpfixObservationDomainId	1.3.6.1.4.1.2272.1.66.1.1.2	8.0
rcIpfixAgingTime	1.3.6.1.4.1.2272.1.66.1.1.3	8.0
rcIpfixCollectorIdTable	1.3.6.1.4.1.2272.1.66.1.2.6	8.0
RcIpfixCollectorIdEntry	1.3.6.1.4.1.2272.1.66.1.2.6.1	8.0
rcIpfixCollectorIdNum	1.3.6.1.4.1.2272.1.66.1.2.6.1.1	8.0
rcIpfixCollectorIdIsReachable	1.3.6.1.4.1.2272.1.66.1.2.6.1.10	8.0
rcIpfixCollectorIdViaNextHopName	1.3.6.1.4.1.2272.1.66.1.2.6.1.11	8.0
rcIpfixCollectorIdExportIntv	1.3.6.1.4.1.2272.1.66.1.2.6.1.12	8.0
rcIpfixCollectorIdInitBurst	1.3.6.1.4.1.2272.1.66.1.2.6.1.13	8.0
rcIpfixCollectorIdRowStatus	1.3.6.1.4.1.2272.1.66.1.2.6.1.14	8.0
rcIpfixCollectorIdAddressType	1.3.6.1.4.1.2272.1.66.1.2.6.1.2	8.0
rcIpfixCollectorIdAddress	1.3.6.1.4.1.2272.1.66.1.2.6.1.3	8.0

Table continues…

Object Name	Object OID	New in VOSS Release
rcIpfixCollectorIdProtocol	1.3.6.1.4.1.2272.1.66.1.2.6.1.4	8.0
rcIpfixCollectorIdSrcPort	1.3.6.1.4.1.2272.1.66.1.2.6.1.5	8.0
rcIpfixCollectorIdDestPort	1.3.6.1.4.1.2272.1.66.1.2.6.1.6	8.0
rcIpfixCollectorIdExporterIpType	1.3.6.1.4.1.2272.1.66.1.2.6.1.7	8.0
rcIpfixCollectorIdExporterIp	1.3.6.1.4.1.2272.1.66.1.2.6.1.8	8.0
rcIpfixCollectorIdState	1.3.6.1.4.1.2272.1.66.1.2.6.1.9	8.0
rcVirtualServiceHypervisorNumCoresRemain	1.6.1.4.1.2272.1.101.1.1.8.1.18	8.0

Table 33: VSP 8000 Series

Object Name	Object OID	New in VOSS Release
rcPortForwardErrorCorrection	1.3.6.1.4.1.2272.1.4.10.1.1.125	8.0
rcPortForwardErrorCorrectionApplicability	1.3.6.1.4.1.2272.1.4.10.1.1.126	8.0

Obsolete MIBs

Table 34: Common

Object Name	Object OID	Obsolete in VOSS Release
rc2kCpuSerialPortDescr	1.3.6.1.4.1.2272.1.100.3.1.2	7.1
rc2kCpuSerialPortMode	1.3.6.1.4.1.2272.1.100.3.1.3	7.1
rc2kCpuSerialPortAdminStatus	1.3.6.1.4.1.2272.1.100.3.1.4	7.1
rc2kCpuSerialPortOperStatus	1.3.6.1.4.1.2272.1.100.3.1.5	7.1
rc2kCpuSerialPortDataBits	1.3.6.1.4.1.2272.1.100.3.1.7	7.1
rc2kCpuSerialPortMyAddr	1.3.6.1.4.1.2272.1.100.3.1.8	7.1
rc2kCpuSerialPortPeerAddr	1.3.6.1.4.1.2272.1.100.3.1.9	7.1
rc2kCpuSerialPortSlipMtu	1.3.6.1.4.1.2272.1.100.3.1.10	7.1

Table continues…

Object Name	Object OID	Obsolete in VOSS Release
rc2kCpuSerialPortSlipTxRxCompress	1.3.6.1.4.1.2272.1.100.3.1.11	7.1
rc2kCpuSerialPortSlipRxCompress	1.3.6.1.4.1.2272.1.100.3.1.12	7.1
rc2kCpuSerialPortPppConfigFile	1.3.6.1.4.1.2272.1.100.3.1.13	7.1