ExtremeSwitching™

Release Notes for VOSS

Release 8.2.5
9036883-00 Rev AE
January 2021

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, 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: https://www.extremenetworks.com/support/policies/open-source-declaration/

Contents

Chapter 1: About this Document

This section discusses the purpose of this document, the conventions used, ways to provide feedback, additional help, and information regarding other Extreme Networks publications.

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.

Table continues…

Icon	Alerts you to...
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.
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>`

Table continues…

Convention	Description
	`<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.
`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

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and software compatibility for Extreme Networks products
Extreme Optics Compatibility
Other resources such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, 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: (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, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions 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

Subscribe 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 (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. Select **Submit**.

Providing Feedback

The Information Development team at Extreme Networks has 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 we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

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 platforms support VOSS 8.2.5:

- 5520 Series
- VSP 4450 Series
- VSP 4900 Series
- VSP 7200 Series
- VSP 7400 Series
- VSP 8000 Series, which includes the VSP 8200 Series and VSP 8400 Series
- XA1400 Series

New Hardware

For VOSS 8.2.5 release with 7 models and 3 VIMs

5520 Series is a new hardware family of switches that supports both ExtremeXOS and VOSS. VOSS 8.2.5 supports the following models:

- 5520-24T: 24 10/100/1000BASE-T full-duplex (FDX), half-duplex (HDX), MACsec-capable ports and 2 QSFP28 Universal Ethernet ports
- 5520-24W: 24 10/100/1000BASE-T FDX/HDX 802.3bt Type 4 PoE MACsec-capable ports and 2 QSFP28 Universal Ethernet ports
- 5520-48T: 48 10/100/1000BASE-T FDX/HDX MACsec-capable ports, and 2 QSFP28 Universal Ethernet ports
- 5520-48W: 48 10/100/1000BASE-T FDX/HDX 802.3bt Type 4 PoE MACsec-capable ports and 2 QSFP28 Universal Ethernet ports
- 5520-12MW-36W: 12 100 Mbps/1 Gbps/2.5 Gbps/5 Gbps 802.3bt Type 4 PoE MACsec-capable ports, 36 10/100/1000BASE-T FDX/HDX 802.3bt Type 4 PoE MACsec-capable ports, and 2 QSFP28 Universal Ethernet ports
- 5520-24X: 24 100/1000BASE-X/10GBASE-X SFP+ ports and 2 QSFP28 Universal Ethernet ports
- 5520-48SE: 48 100/1000BASE-X MACsec-capable SFP ports and 2 QSFP28 Universal Ethernet ports

In addition to the fixed ports, all models provide console interface ports (one micro Type B USB and one RJ-45), one RJ-45 out-of-band (OOB) management port (10/100/1000), two USB ports for removable storage, one VIM slot, and hot-swappable, redundant power supplies and fan units.

Each model provides one Versatile Interface Module (VIM) slot. You can install any one of the following VIMs in the VIM slot to provide flexible linkage to other switches or devices over a range of media:

- 5520-VIM-4X: Four 1 Gbps/10 Gbps SFP+ ports
- 5520-VIM-4XE: Four 1 Gbps/10 Gbps LRM/MACsec-capable SFP+ ports
- 5520-VIM-4YE: Four 10 Gbps/25 Gbps MACsec-capable SFP28 ports

New Transceivers and Components

VOSS 8.2.5 introduces support for the following optical devices. They have been consolidated and qualified for use in Extreme Networks platforms, with enhanced diagnostics for transceivers. Enhanced diagnostic information includes power-on counters, comparison statistics for actual Tx and Rx dB values versus low alarm values, and the associated logging for these enhancements.

- 40 Gb cable
  - 40 Gb active optical breakout cable, QSFP+ to 4xSFP+, 20 meter (10GB-4-F20-QSFP) (5520 Series)
- 100 Gb cables

  Note:

  Supported on 5520 stacking ports only. The cables must have 4x25 channelization, and there must be an MLT for the four channels on both ends.

  - 100 Gb passive DAC QSFP28, 0.5 meters (10410) (5520 Series)
  - 100 Gb passive breakout DAC, QSFP28 to 2xQSFP28, 1 meter (10426) (5520 Series)
  - 100 Gb passive breakout DAC, QSFP28 to 2xQSFP28, 3 meters (10428) (5520 Series)
  - 100 Gb passive breakout DAC, QSFP28 to 2xQSFP28, 5 meters (10429) (5520 Series)
  - 100 Gb active optical cable TAA, QSFP28, 7 meters (10435) (5520 Series)

Extreme Networks might announce support for additional optical components in the future. For a complete and current list of supported optical components, see the Extreme Optics website.

New Software Features in VOSS 8.2.5

The following sections describe what is new in VOSS 8.2.5.

Support for Universal Hardware: 5520 Series Switches

ExtremeSwitching 5520 Series is a family of high-performance aggregation switches. The 5520 Series universal hardware provides end-to-end secure network segmentation, in addition to advanced policy capabilities, and offers a user-selectable choice of Extreme's flagship switch operating systems.

The 5520 Series includes 24- and 48-port 1 Gigabit models, 1/2.5/5 Gigabit multi-rate models, as well as a 24-port 10 Gigabit model. The family also offers 30/60/90W PoE, and supports 10G and 25G modular uplinks for flexible linkage to other switches or devices over a range of media.

The 10/100/1000Base-T ports on the 5520-24W/12MW-36W/48T/48W models can operate in half-duplex mode when operating at 10Mbps or 100Mbps. Half-duplex is not supported on these ports when operating at 1Gbps.

ExtremeSwitching 5520 Series switches support unified licensing, so that you can use them with multiple Extreme Networks operating systems, including VOSS 8.2.5. For details about acquiring and activating licenses, see Licensing for Universal Hardware (5520 Series) on page 95.

For information about selecting the operating system for a 5520 Series switch and changing your selection after initial activation, see Switch Operating System Selection for Universal Hardware.

Zero Touch Provisioning Plus (ZTP+) for On-boarding with Extreme Management Center 8.5

In VOSS 8.2.5, ZTP+ functionality is extended to Extreme Management Center version 8.5.

Zero Touch Provisioning Plus (ZTP+) provides Extreme Management Center connectivity to VOSS switches. With zero touch functionality, VOSS switches automatically connect and start onboarding to Extreme Management Center the moment they are able to obtain an IP address from the network.

ZTP+ enables you to deploy and configure VOSS switches in Extreme Management Center with minimal server configuration and intervention. ZTP+ enabled switches send information, such as the serial number, software version, MAC, management IP, and port information to Extreme Management Center automatically.

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

DEMONSTRATION FEATURE - Fabric IPsec Gateway on VSP 4900 Series

The Fabric IPsec Gateway feature introduces a new Virtual Machine that supports aggregation of Fabric Extend Tunnels with fragmentation, reassembly, and Internet Protocol Security (IPsec) encryption functions for VSP switches.

Starting with VOSS 8.2.5, the Fabric IPsec Gateway feature is available for VSP 4900 Series switches. The feature continues to be available for VSP 7400 Series switches.

For more information, see:

- Configuring Fabric Basics and Layer 2 Services for VOSS
- Configuring User Interfaces and Operating Systems 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, such as, `VSP4K4.1.0.0.tgz`. In VOSS 4.2.1 and later, image filenames start with VOSS, such as, `VOSS8K4.2.1.0.tgz`.

Prior to VOSS 8.1, software image filenames contained either a product family, or a product platform, depending on the product. In VOSS 8.1 and later, all software image filenames contain a product platform, to more accurately and consistently describe the switches that the software applies to.

In VOSS 8.1 and later, when extracting the software image file, the extraction process appends the software version portion of the extracted filenames to include the final full software version. (For example, extracting **`VOSS8400.8.2.5.0.tgz`** results in a software file named **`VOSS8400.8.2.5.0.GA`**.) Ensure that you specify the final full software version (in this case, **`8.2.5.0.GA`**) when using CLI commands that include the software version, such as activating or removing the software.

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: 5520 Series Software Filenames and Sizes

Description	File	Size
SHA512 Checksum files	5520.8.2.5.0.sha512	1,518 bytes
MD5 Checksum files	5520.8.2.5.0.md5	558 bytes
MIB - supported object names	5520.8.2.5.0_mib_sup.txt	1,435,203 bytes
MIB - zip file of all MIBs	5520.8.2.5.0_mib.zip	1,172,885 bytes
MIB - objects in the OID compile order	5520.8.2.5.0_mib.txt	7,793,457 bytes
EDM Help files	VOSSv820_HELP_EDM_gzip.zip	4,414,827 bytes
Logs reference	5520.8.2.5.0_edoc.tar	66,529,280 bytes
Software image	5520.8.2.5.0.voss	98,740,101 bytes
Open source software - Master copyright file	5520.8.2.5.0_oss-notice.html	2,766,416 bytes
YANG model	restconf_yang.tgz	506,020 bytes

Table 4: VSP 4450 Series Software Filenames and Sizes

Description	File	Size
SHA512 Checksum files	VOSS4400.8.2.5.0.sha512	1,549 bytes
MD5 Checksum files	VOSS4400.8.2.5.0.md5	589 bytes
MIB - supported object names	VOSS4400.8.2.5.0_mib_sup.txt	1,413,418 bytes
MIB - zip file of all MIBs	VOSS4400.8.2.5.0_mib.zip	1,172,885 bytes
MIB - objects in the OID compile order	VOSS4400.8.2.5.0_mib.txt	7,793,457 bytes
EDM Help files	VOSSv820_HELP_EDM_gzip.zip	4,414,827 bytes
Logs reference	VOSS4400.8.2.5.0_edoc.tar	66,529,280 bytes
Software image	VOSS4400.8.2.5.0.tgz	112,236,977 bytes
Open source software - Master copyright file	VOSS4400.8.2.5.0_oss-notice.html	2,766,416 bytes
YANG model	restconf_yang.tgz	506,020 bytes

Table 5: VSP 4900 Series Software Filenames and Sizes

Description	File	Size
SHA512 Checksum files	VOSS4900.8.2.5.0.sha512	1,701 bytes
MD5 Checksum files	VOSS4900.8.2.5.0.md5	645 bytes
MIB - supported object names	VOSS4900.8.2.5.0_mib_sup.txt	1,436,064 bytes
MIB - zip file of all MIBs	VOSS4900.8.2.5.0_mib.zip	1,172,885 bytes
MIB - objects in the OID compile order	VOSS4900.8.2.5.0_mib.txt	7,793,457 bytes
EDM Help files	VOSSv820_HELP_EDM_gzip.zip	4,414,827 bytes
Logs reference	VOSS4900.8.2.5.0_edoc.tar	66,529,280 bytes
Software image	VOSS4900.8.2.5.0.tgz	244,685,067 bytes
Open source software - Master copyright file	VOSS4900.8.2.5.0_oss-notice.html	2,766,416 bytes
YANG model	restconf_yang.tgz	506,020 bytes
Third Party Virtual Machine (TPVM)	TPVM_4900_8.2.0.0.img	1,677,066,240 bytes

Table 6: VSP 7200 Series Software Filenames and Sizes

Description	File	Size
SHA512 Checksum files	VOSS7200.8.2.5.0.sha512	1,549 bytes
MD5 Checksum files	VOSS7200.8.2.5.0.md5	589 bytes
MIB - supported object names	VOSS7200.8.2.5.0_mib_sup.txt	1,379,657 bytes

Table continues…

Description	File	Size
MIB - zip file of all MIBs	VOSS7200.8.2.5.0_mib.zip	1,172,885 bytes
MIB - objects in the OID compile order	VOSS7200.8.2.5.0_mib.txt	7,793,457 bytes
EDM Help files	VOSSv820_HELP_EDM_gzip.zip	4,414,827 bytes
Logs reference	VOSS7200.8.2.5.0_edoc.tar	66,529,280 bytes
Software image	VOSS7200.8.2.5.0.tgz	126,617,891 bytes
Open source software - Master copyright file	VOSS7200.8.2.5.0_oss-notice.html	2,766,416 bytes
YANG model	restconf_yang.tgz	506,020 bytes

Table 7: VSP 7400 Series Software Filenames and Sizes

Description	File	Size
SHA512 Checksum files	VOSS7400.8.2.5.0.sha512	1,857 bytes
MD5 Checksum files	VOSS7400.8.2.5.0.md5	705 bytes
MIB - supported object names	VOSS7400.8.2.5.0_mib_sup.txt	1,430,261 bytes
MIB - zip file of all MIBs	VOSS7400.8.2.5.0_mib.zip	1,172,885 bytes
MIB - objects in the OID compile order	VOSS7400.8.2.5.0_mib.txt	7,793,457 bytes
EDM Help files	VOSSv820_HELP_EDM_gzip.zip	4,414,827 bytes
Logs reference	VOSS7400.8.2.5.0_edoc.tar	66,529,280 bytes
Software image	VOSS7400.8.2.5.0.tgz	244,346,473 bytes
Open source software - Master copyright file	VOSS7400.8.2.5.0_oss-notice.html	2,766,416 bytes
YANG model	restconf_yang.tgz	506,020 bytes
Third Party Virtual Machine (TPVM)	TPVM_7400_8.2.0.0.img	1,677,066,240 bytes
Fabric IPsec Gateway	FIGWVM_7400_8.2.0.0.qcow2	1,970,339,840 bytes

Table 8: VSP 8200 Series Software Filenames and Sizes

Description	File	Size
SHA512 Checksum files	VOSS8200.8.2.5.0.sha512	1,549 bytes
MD5 Checksum files	VOSS8200.8.2.5.0.md5	589 bytes
MIB - supported object names	VOSS8200.8.2.5.0_mib_sup.txt	1,379,657 bytes
MIB - zip file of all MIBs	VOSS8200.8.2.5.0_mib.zip	1,172,885 bytes
MIB - objects in the OID compile order	VOSS8200.8.2.5.0_mib.txt	7,793,457 bytes
EDM Help files	VOSSv820_HELP_EDM_gzip.zip	4,414,827 bytes

Table continues…

Description	File	Size
Logs reference	VOSS8200.8.2.5.0_edoc.tar	66,529,280 bytes
Software image	VOSS8200.8.2.5.0.tgz	126,621,654 bytes
Open source software - Master copyright file	VOSS8200.8.2.5.0_oss-notice.html	2,766,416 bytes
YANG model	restconf_yang.tgz	506,020 bytes

Table 9: VSP 8400 Series Software Filenames and Sizes

Description	File	Size
SHA512 Checksum files	VOSS8400.8.2.5.0.sha512	1,549 bytes
MD5 Checksum files	VOSS8400.8.2.5.0.md5	589 bytes
MIB - supported object names	VOSS8400.8.2.5.0_mib_sup.txt	1,379,657 bytes
MIB - zip file of all MIBs	VOSS8400.8.2.5.0_mib.zip	1,172,885 bytes
MIB - objects in the OID compile order	VOSS8400.8.2.5.0_mib.txt	7,793,457 bytes
EDM Help files	VOSSv820_HELP_EDM_gzip.zip	4,414,827 bytes
Logs reference	VOSS8400.8.2.5.0_edoc.tar	66,529,280 bytes
Software image	VOSS8400.8.2.5.0.tgz	188,111,817 bytes
Open source software - Master copyright file	VOSS8400.8.2.5.0_oss-notice.html	2,766,416 bytes
YANG model	restconf_yang.tgz	506,020 bytes

Table 10: XA1400 Series Software Filenames and Sizes

Description	File	Size
SHA512 Checksum files	VOSS1400.8.2.5.0.sha512	1,401 bytes
MD5 Checksum files	VOSS1400.8.2.5.0.md5	537 bytes
MIB - supported object names	VOSS1400.8.2.5.0_mib_sup.txt	1,086,794 bytes
MIB - zip file of all MIBs	VOSS1400.8.2.5.0_mib.zip	1,172,885 bytes
MIB - objects in the OID compile order	VOSS1400.8.2.5.0_mib.txt	7,793,457 bytes
EDM Help files	VOSSv820_HELP_EDM_gzip.zip	4,414,827 bytes
Logs reference	VOSS1400.8.2.5.0_edoc.tar	66,529,280 bytes
Software image	VOSS1400.8.2.5.0.tgz	322,542,599 bytes
Open source software - Master copyright file	VOSS1400.8.2.5.0_oss-notice.html	2,766,416 bytes

Chapter 3: Upgrade and Downgrade Considerations

Do not upgrade to VOSS 8.2.5.0 if you are using Distributed Virtual Routing (DvR) in your network.

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

- IPv6:
  - Notes for systems using IPv6 static neighbors
  - Considerations for IPv6 VRRP or DHCP Relay configurations saved in VOSS 4.1 or 4.2
- Fabric:
  - Pre-upgrade instructions for IS-IS metric type
  - Upgrade considerations for IS-IS enabled links with HMAC-MD5 authentication
  - The following releases included modified Zero Touch Fabric Configuration support that impacts upgrades from earlier releases: VOSS 7.1.3 and later, VOSS 8.0.6 and later, and VOSS 8.1 and later.
- Upgrade considerations regarding MACsec replay-protect configuration
- Upgrade support for the nni-mstp boot configuration flag
- TACACS+ upgrade consideration
- Considerations for switches running an Extreme Integrated Application Hosting virtual service configured prior to VOSS 8.0.5.
- Considerations for VLANs or MLTs where the VLAN or MLT name uses all numbers.
- Considerations for digital certificates configured prior to VOSS 8.1.
- Considerations for Fast PoE and Perpetual PoE features configured prior to VOSS 8.1.5.

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

Supported Upgrade Paths

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

Supported Upgrade Path for all switches

Validated upgrade paths are:

- 8.2 to 8.2.5
- 8.1.5 to 8.2.5
- 8.1.x to 8.2.5
- 8.0.x to 8.2.5
- 7.1.x to 8.2.5

Switches using earlier software releases must upgrade to one of these releases first before upgrading to 8.2.5.

Switches can be upgraded using one of the following two options:

1. Switches that will not use Zero Touch Deployment with ExtremeCloud™ IQ should upgrade to 8.2.5 by performing these steps:
   - Migrate the Management IP address. For more information, see Administering VOSS.
   - Upgrade to Release 8.2.5 from one of the previously described releases.
   - Continue to use the previous switch configuration.
2. Switches that will use Zero Touch Deployment with ExtremeCloud™ IQ should upgrade to 8.2.5 by performing the following steps.

   Important:

   When you perform these steps, any prior configuration for this switch is lost.

   - Upgrade to Release 8.2.5 from one of the previously described releases.
   - Delete the primary and secondary configuration files.
   - Reboot the switch.

   Performing these steps will result in a switch with a Zero Touch Deployment configuration with the following characteristics:

   - All devices
     - VLAN 4048 is the designated Management VLAN.
     - SSH is enabled.
     - DHCP client is enabled and set to cycle.
   - All VSP devices
     - All ports are enabled and members of the Management VLAN.
     - VLAN 4048 and all interfaces are set to `private-vlan isolated`.
     - VLAN 4049 is configured as a secondary VLAN for all ports as required by Private VLAN ports.
   - XA1400 Series devices
     - Ports 1/1 to 1/7 are disabled and members of VLAN 1.

- Port 1/8 is enabled and a member of VLAN 4048.

After the switch reboots in the Zero Touch Deployment configuration, the DHCP client and IQAgent are enabled. The DHCP client obtains an IP address for the switch, DNS discovery is used to discover a Domain Name Server, and the switch attempts to connect to ExtremeCloud™ IQ. If the switch has been properly onboarded in ExtremeCloud™ IQ, it can now be monitored and configured in ExtremeCloud™ IQ. Additional operational configuration is performed using EDM or the CLI.

Downgrade Considerations

Save the switch configuration before upgrading to VOSS 8.2.5. VOSS 8.2.5 contains significant enhancements which cannot be used in previous software versions. Downgrading to an earlier release will require a compatible configuration file.

Segmented Management Instance Migration

Important:

VOSS 8.2 introduced changes to Segmented Management Instance that required migration of legacy management interfaces. Before you upgrade to VOSS 8.2 or later from an earlier release, you must consider your management interface configuration and migration scenario requirements. Backup and save your configuration files off the switch before upgrading to this release.

If the switch already runs VOSS 8.2 or later, you can ignore this section.

Note:

Management interface access to the switch can be lost if you do not perform the applicable migration scenarios before upgrading to this release. Loss of management access after an upgrade can result in an automatic roll-back to the previous software version.

You must perform a manual software commit after upgrading from VOSS Release 8.1.5.0 or earlier to VOSS 8.2 or later. Management interface access is required to input the `software commit` CLI command within 10 minutes after the upgrade. If the time expires the system initiates an automatic roll-back to the previous release.

You must ensure the switch runs one of the following VOSS releases before you upgrade to VOSS 8.2 or later:

- VOSS 8.1.0.0 or later for switches running VOSS 8.1.x releases.
- VOSS 8.0.1.0 or later for switches running VOSS 8.0.x releases.
- VOSS 7.1.3.0 or later for switches running VOSS 7.1.x releases.

Note:

If the network environment must migrate static IPv6 routes, the switches must run VOSS Release 8.1.2.0 or later before you upgrade to VOSS 8.2 or later.

You must consider the following legacy management interface migration scenarios before you upgrade to VOSS 8.2 or later:

Table 11: Management Interface Migration Scenarios

Mgmt Interface	Mgmt Scenario	Migration Description
DVR leaf	Automatic migration during upgrade.	DvR leaf settings migrate automatically during the software upgrade process. **Note:** Leaf nodes only support the management CLIP as part of the Global Routing Table (GRT).
OOB	Automatic migration during upgrade.	Out-of-Band management settings migrate automatically during the software upgrade process.
CLIP	Specify a Circuitless IP (CLIP) interface for migration to management interface before upgrading.	Use the **`migrate-to-mgmt`** command in the Loopback interface configuration CLI to specify the CLIP interface for management before starting the software upgrade process. The loopback IP to migrate can include the configured ISIS IP shortcuts. Save the configuration before upgrading. A Fabric or legacy Layer 3 network typically uses the CLIP management interface.
VLAN	Specify a VLAN interface for migration to management interface before upgrading.	Use the **`migrate-to-mgmt`** command in the VLAN interface configuration CLI mode to specify the VLAN interface for management before starting the software upgrade process. Save the configuration before upgrading. A Layer 2 network typically uses the VLAN management interface, or for restricting management access to a specific subnet or I-SID.

For more information about Segmented Management Instance migration, see Administering VOSS.

Segmented Management Instance Migration and DvR

Starting with VOSS Release 8.2, VSP devices can be managed by a CLIP/Loopback IP address that is assigned to a virtual router and forwarder (VRF) that is not in the Global Routing Table (GRT). When you convert a VSP switch from a regular backbone edge bridge (BEB) to a DvR leaf device by setting the DvR leaf boot flag, you must assign the management CLIP to the GRT. If you assign the management CLIP to a VRF, the device will not be reachable after the migration because the management CLIP cannot be migrated.

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.

In order to minimize the impact of this incompatibility and the resulting loss of connectivity between DvR Controller nodes and Leaf nodes, upgrade all DvR Leaf nodes first. After you upgrade all Leaf nodes, upgrade the Controller nodes, which restores DvR connectivity to the already upgraded Leaf nodes.

Important:

During the 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 this upgrade order, 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. If vIST is configured, use the **`no dvr leaf virtual-ist`** command on the Leaf nodes.
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 23
- Option 2: Enable Dynamic Nickname Assignment on page 24
- Option 3: Enable Zero Touch Fabric Connect configuration on page 25
- Option 4: Disable Zero Touch Fabric Connect configuration and Dynamic Nickname Assignment on page 25

Note:

The following releases included modified Zero Touch Fabric Configuration support that impacts upgrades from earlier releases: VOSS 7.1.3 and later, VOSS 8.0.6 and later, and VOSS 8.1 and later.

- VOSS 7.1.3 and later
- VOSS 8.0.6 and later
- VOSS 8.1 and later

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.

5520 Series Hardware

Part number	Model	Initial release	Supported new feature release
			8.2.5
5520-24T	5520-24T switch	8.2.5	Y
5520-24W	5520-24W switch	8.2.5	Y
5520-48T	5520-48T switch	8.2.5	Y
5520-48W	5520-48W switch	8.2.5	Y
5520-12MW-36W	5520-12MW-36W switch	8.2.5	Y
5520-24X	5520-24X switch	8.2.5	Y
5520-48SE	5520-48SE	8.2.5	Y
Versatile Interface Modules (VIMs)			
5520-VIM-4X	5520-VIM-4X	8.2.5	Y
5520-VIM-4XE	5520-VIM-4XE	8.2.5	Y
5520-VIM-4YE	5520-VIM-4YE	8.2.5	Y

5520 Series Operational Notes

Information to be added.

Versatile Interface Module Operational Notes

The following table summarizes the operational capabilities of the various VIMs:

Table 12: 5520-VIM Matrix

	5520-VIM-4X	5520-VIM-4XE	5520-VIM-4YE
Operational speeds	1Gbps & 10Gbps	1Gbps & 10Gbps	10Gbps & 25Gbps

Table continues…

	5520-VIM-4X	5520-VIM-4XE	5520-VIM-4YE
PHY present	No	Yes	Yes
1000BASE-T & 10GBASE-T	10GBASE-T only	Both	10GBASE-T only
Mixed speeds	1Gbps & 10Gbps	1Gbps & 10Gbps	Mixed speeds not supported
1G Auto-negotiation	Disabled	Disabled	Disabled
10G Auto-negotiation	Disabled	Disabled	Disabled
25G Auto-negotiation			Enabled for DAC Disabled for Fiber
FEC	Not supported	Not supported	Auto-FEC enabled for DAC and Fiber
MACsec	Not supported	128/256 bit	128/256 bit

Operational Notes for VIMs

The IEEE 802.3by requirement for 25 Gb is that any transceiver or DAC 3 meters or longer, requires the use of forward error correction (FEC). Because the 5520-VIM-4X and 5520-VIM-4XE do not support FEC, note the following considerations for proper operation with these VIMs:

- Supported 25 Gb optics:
  - PN: 10502 - 25GBASE-SR (FEC-Lite): Up to 30 m for OM3, up to 40 m for OM4
- Supported 25 Gb DACs:
  - 10520 25G SFP28 Cable (1 m)
- You must disable Auto-Negotiation and FEC on any VSP 7400 Series device that is connected to either of these VIMS.

If you use an unsupported 25 Gb transceiver, you might experience CRC or link flap errors.

VSP 4000 Series Hardware

Part number	Model number	Initial release	Supported new feature release				
			8.1	8.1.1	8.1.5	8.2	8.2.5
EC4400004-E6	VSP 4450GSX-DC	4.0.50	Y	Y	Y	Y	Y
EC4400A03-E6	VSP 4450GTX-HT-PWR+	4.0.50	Y	Y	Y	Y	Y
EC4400A05-E6	VSP 4450GSX-PWR+	4.0	Y	Y	Y	Y	Y

Table continues…

Part number	Model number	Initial release	Supported new feature release				
			8.1	8.1.1	8.1.5	8.2	8.2.5
EC4400A05-E6GS	VSP 4450GSX-PWR+ TAA Compliant	4.0.50	Y	Y	Y	Y	Y
EC4800078-E6	VSP 4850GTS-DC	3.0	N	N	N	N	N
EC4800A78-E6 EC4800A78-E6GS	VSP 4850GTS	3.0	N	N	N	N	N
EC4800A88-E6 EC4800A88-E6GS	VSP 4850GTS-PWR+	3.0	N	N	N	N	N

VSP 4000 Series Operational Notes

- **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.

- On a VSP 4450 Series switch, when making the initial connection to the two 10 Gbps SFP+ ports with MACsec-capable PHY (ports 49 and 50), the remote device flaps two times before remaining up due to the MACsec probing done by the VSP 4450 Series switch.

VSP 4900 Series Hardware

Part number	Model number	Initial release	Supported new feature release			
			8.1.1	8.1.5	8.2	8.2.5
VSP4900-48P	VSP4900-48P	8.1	Y	Y	Y	Y
VSP4900-12MXU-12XE	VSP4900-12MXU-12XE	8.1.5	N	Y	Y	Y
VSP4900-24S	VSP4900-24S	8.1.5	N	Y	Y	Y
VSP4900-24XE	VSP4900-24XE	8.1.5	N	Y	Y	Y
Versatile Interface Modules (VIM) **Note:** Ensure the switch runs, at a minimum, the noted initial software release before you install a VIM.						
VIM5-4X	VIM5-4X	8.1	Y	Y	Y	Y

Table continues…

Part number	Model number	Initial release	Supported new feature release			
			8.1.1	8.1.5	8.2	8.2.5
VIM5-4XE	VIM5-4XE	8.1	Y	Y	Y	Y
VIM5-2Y	VIM5-2Y	8.1	Y	Y	Y	Y
VIM5-4YE	VIM5-4YE	8.1	Y	Y	Y	Y
VIM5-2Q	VIM5-2Q	8.1	Y	Y	Y	Y
VIM5-4Y	VIM5-4Y	8.1.5	N	Y	Y	Y

VSP 4900 Series Operational Notes

VSP4900-24S fixed ports operate at 1 Gbps. If you connect a 10 Gbps DAC/SFP+ to a VSP4900-24S 1 Gbps fixed port, the system displays the following error message:

```
10Gb optical module inserted in 1Gb only port nn. Not supported.
```

Although the link successfully comes up, the operational speed shows as 10 Gbps instead of 1 Gbps. This scenario occurs when a 10 Gbps DAC/SFP+ is used to make any of the following connections from a VSP4900-24S 1 Gbps fixed port:

- a VSP4900-24S to VSP4900-24S loopback connection
- a VSP4900-24S connected to another VSP4900-24S
- a VSP4900-24S connected to a VSP 4450GSX

Versatile Interface Module Operational Notes

The following table summarizes the operational capabilities of the various VIMs:

	VIM5-4X	VIM5-4XE	VIM5-2Y	VIM5-4YE	VIM5-4Y	VIM5-2Q
Number of supported ports for VSP4900-48P and VSP4900-24S	4	4	2	2	2	1
Number of supported ports for VSP4900-24XE and VSP4900-12MXU-12XE	4	4	2	4	4	2
Port speeds	• 1 Gbps • 10 Gbps	• 1 Gbps • 10 Gbps	• 10 Gbps or • 25 Gbps All ports must operate at either 10 Gbps or 25 Gbps (default)	• 10 Gbps or • 25 Gbps All ports must operate at either 10 Gbps or 25 Gbps (default)	• 10 Gbps or • 25 Gbps All ports must operate at either 10 Gbps or 25 Gbps (default)	• 40 Gbps • 10 Gbps (with channelization)
PHY present	No	Yes	Yes	Yes	Yes	No
Copper transceiver support (1 Gbps/10 Gbps)	10GBASE-T only	Both	10GBASE-T only	10GBASE-T only	10GBASE-T only	Not applicable

Table continues…

	VIM5-4X	VIM5-4XE	VIM5-2Y	VIM5-4YE	VIM5-4Y	VIM5-2Q
MACsec	Not supported	128/256 bit	Not supported	128/256 bit	Not supported	Not supported
Forward Error Correction (FEC)	Not supported	Not supported	Not supported	Default is Auto-FEC - FEC Auto, CL108, CL91, CL74 and No FEC supported	Not supported	Not supported
1 Gbps Auto-Negotiation	Disabled	Enabled	Not applicable	Not applicable	Not applicable	Not applicable
10 Gbps Auto-Negotiation	Disabled	Disabled	Disabled	Disabled	Disabled	Not applicable
25 Gbps Auto-Negotiation	Not applicable	Not applicable	Disabled	• Enabled for DACs • Disabled for AOCs, optical transceivers	Disabled	Not applicable
Note: Auto-Negotiation values are automatically set based on the type of transceiver detected.						

VIM5-2Y and VIM5-4Y Operational Notes

Note:
VIM5-2Y and VIM5-4Y are in end-of-sale status.

The IEEE 802.3by requirement for 25 G is that any transceiver or DAC 3 meters or longer, requires the use of forward error correction (FEC). Because the VIM5-2Y and VIM5-4Y do not support FEC, note the following considerations for proper operation with these VIMs:

- Supported 25 G optics:
  - PN: 10502 - 25GBASE-SR (FEC-Lite): up to 30 m for OM3, up to 40 m for OM4
- Supported 25 G DACs:
  - 10520 25G SFP28 Cable (1 m)
- You must disable Auto-Negotiation and FEC on any VSP 7400 Series device that is connected to either of these VIMs.

You might experience CRC or link flap errors by using an unsupported 25 G transceiver.

VSP 7200 Series Hardware

Part number	Model number	Initial release	Supported new feature release				
			8.1	8.1.1	8.1.5	8.2	8.2.5
EC720001F-E6	VSP 7254XSQ DC (front to back airflow)	4.2.1	Y	Y	Y	Y	Y
EC7200A1B-E6 (back-to-front airflow) EC7200A1F-E6 (front-to-back airflow)	VSP 7254XSQ	4.2.1	Y	Y	Y	Y	Y
EC720002F-E6	VSP 7254XTQ DC (Front to back airflow)	4.2.1	Y	Y	Y	Y	Y
EC7200A2B-E6 (back-to-front airflow) EC7200A2F-E6 (front-to-back airflow)	VSP 7254XTQ	4.2.1	Y	Y	Y	Y	Y
EC7200A3B-E6 (back-to-front airflow) EC7200A3F-E6 (front-to-back airflow)	VSP 7254XSQ Port Licensed	5.1	Y	Y	Y	Y	Y
EC7200A4B-E6 (back-to-front airflow) EC7200A4F-E6 (front-to-back airflow)	VSP 7254XTQ Port Licensed	5.1	Y	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 that require electronic dispersion compensation (EDC) for proper operation 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				
			8.1	8.1.1	8.1.5	8.2	8.2.5
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	Y	Y	Y	Y
VSP7400-48Y-8C (no power supplies or fans) VSP7400-48Y-8C-AC-F (front-to-back airflow) VSP7400-48Y-8C-AC-R (back-to-front airflow)	VSP 7400-48Y	8.0.5	Y	Y	Y	Y	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 that require electronic dispersion compensation (EDC) for proper operation 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 (low) or ports 29, 30, 31, and 32 (high) are reserved for internal use when certain features, including Fabric Connect, are used. For a full list of the features, refer to Administering VOSS.
- 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.

The following list provides operational notes for VSP 7400-48Y.

- Ports 55 and 56 (low) or ports 53, 54, 55, and 56 (high) are reserved for internal use when certain features, including Fabric Connect, are used. For a full list of the features, refer to Administering VOSS.
- 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+.
- The SFP28 ports support the use of SFP28, SFP, and SFP+ transceivers.
  - The software detects the transceiver type and sets the port speed as either 25 Gbps for SFP28,.1 Gbps for SFP, or 10 Gbps for SFP+.
  - Auto-Negotiation is not supported when a 25 Gbps port operates at 1 Gbps. The following log message displays on the switch: `Auto-Negotiation enabled but not applied to port 1/1 since 1G transceiver is present..`
- Channelization is not supported. As a result, you cannot use the following optical components:
  - 40 Gbps or 100 Gbps breakout cables
  - QSFP28 to SFP28 Adapter (PN: 10506)

VSP 8000 Series Hardware

Part number	Model number	Initial release	Supported new feature release				
			8.1	8.1.1	8.1.5	8.2	8.2.5
EC8200A01-E6 EC8200A01-E6GS	VSP 8284XSQ	4.0	Y	Y	Y	Y	Y
EC8200001-E6	VSP 8284XSQ DC	4.0.50	Y	Y	Y	Y	Y
EC8400001-E6	VSP 8404 DC	4.2.1	Y	Y	Y	Y	Y
EC8400A01-E6 EC8200A01-E6GS	VSP 8404	4.2	Y	Y	Y	Y	Y
EC8400002-E6	VSP 8404C DC	5.3	Y	Y	Y	Y	Y
EC8400A02-E6 EC8200A02-E6GS	VSP 8404C	5.3	Y	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	8424XS	4.2	Y	Y	Y	Y	Y

Table continues…

Part number	Model number	Initial release	Supported new feature release				
			8.1	8.1.1	8.1.5	8.2	8.2.5
EC8404001-E6GS							
EC8404002-E6 EC8404002-E6GS	8424XT	4.2	Y	Y	Y	Y	Y
EC8404003-E6 EC8404003-E6GS	8408QQ	4.2	Y	Y	Y	Y	Y
EC8404005-E6 EC8404005-E6GS	8418XSQ	4.2	Y	Y	Y	Y	Y
EC8404006-E6 EC8404006-E6GS	8418XTQ	5.0	Y	Y	Y	Y	Y
EC8404007-E6 EC8404007-E6GS	8424GS	5.0	Y	Y	Y	Y	Y
EC8404008-E6 EC8404008-E6GS	8424GT	5.0	Y	Y	Y	Y	Y
EC8404009-E6 EC8404009-E6GS	8402CQ Supported in VSP 8404C only	5.3	Y	Y	Y	Y	Y

XA1400 Series Hardware

Part number	Model number	Initial release	Supported new feature release				
			8.1.1	8.1.50	8.1.5	8.2	8.2.5
XA1440	ExtremeAccess Platform 1440 (XA1440)	8.0.50	Y	Y	Y	Y	Y
XA1480	ExtremeAccess Platform 1480 (XA1480)	8.0.50	Y	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.

Compatibility for Extreme Networks SFP, SFP+, QSFP+, and QSFP28 transceiver modules with the VOSS-capable switches	Extreme Optics website
Descriptions of Extreme Networks optical transceivers and components	*Extreme Networks Pluggable Transceivers Installation Guide*

Auto-Negotiation

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

When you use a 1 Gb SFP transceiver on a 10 Gb SFP+ port, ensure that auto-negotiation is enabled. Note, however, the following special considerations:

- If you use 1 Gb SFP transceivers on a VSP 4000 Series switch that is connected to third-party switches, you must have auto-negotiation enabled at all times. This applies to SFP transceivers installed in either 1 Gb SFP ports or 10 Gb SFP+ ports.
- Auto-negotiation is not supported for the VSP 7254XSQ. On the VSP 7254XSQ, if you are using a 1 Gb SFP module, the link can be established only when auto-negotiation is disabled at the remote device. Also note that, because the SFP+ ports on the VSP 7254XSQ support only 1 Gb and 10 Gb speeds, the 1000BASE-T SFP module (part no. AA1419043-E6 or 10070H) can operate only at 1 Gb.
- For 1000BASE-T SFP transceivers, we recommend performing custom auto-negotiation at the remote native copper port. This can prevent connections from failing if the speed or duplex negotiation changes.

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 platform. This section lists the power supplies and indicates the compatible platforms.

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

- ExtremeSwitching 5520 Series Hardware Installation Guide
- Installing the Virtual Services Platform 4850GTS Series
- Installing the Virtual Services Platform 4450GTX-HT-PWR+
- Installing the Virtual Services Platform 4450GSX-PWR+
- VSP 4900 Series Switches: Hardware Installation Guide
- Installing the Virtual Services Platform 7200 Series
- VSP 7400 Series Switches: Hardware Installation Guide
- Installing the Virtual Services Platform 8000 Series
- XA1400 Series Switches: Hardware Installation Guide

Note:

In the following table for 5520 Series power supplies:

- All 5520-compatible power supplies have front-to-back ventilation airflow.
- Each power supply has a keyed power inlet (C16) that requires a notched (C15) power cord.

Table 13: 5520 Series Power Supplies

Platform	350 W AC PSU-FB 10953	715 W AC PSU-FB 10951	1100 W AC PSU-FB 10941	2000 W AC PSU-FB XN-ACPWR-2000W-F
5520-24T	Y	—	—	—
5520-24W	—	Y	Y	Y
5520-24X	Y	—	—	—
5520-12MW-36W	—	Y	Y	Y
5520-48T	Y	—	—	—
5520-48W	—	Y	Y	Y
5520-48SE	Y	—	—	—

Table 14: VSP 4000 Series Power Supplies

Platform	300 W AC AL1905A08-E5	300 W DC AL1905005-E5	1000 W AC AL1905A21-E6	1000 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 15: VSP 4900 Series Power Supplies

Platform	350 W AC 10953	715 W AC 10951	1100 W AC 10941	2000 W AC XN-ACPWR-2000W-F
VSP4900-48P	—	Y	Y	Y
VSP4900-12MXU-12XE	—	Y	Y	Y
VSP4900-24XE	Y	—	—	—
VSP4900-24S	Y	—	—	—

Table 16: 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
VSP 7254XSQ front-to-back	Y	—	—	—	—	—
VSP 7254XSQ back-to-front	—	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 7254XTQ front-to-back	—	—	—	Y	—	—
VSP 7254XTQ back-to-front	—	—	—	—	Y	—
VSP 7254XSQ DC	—	—	—	—	—	Y
VSP 7254XTQ DC	—	—	—	—	—	Y

The following table for VSP 7400 Series includes the orderable part number as well as the model number or model name, as it is displayed on the power supply.

Table 17: 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
Model Number/ Model Name	700-013684-0100/ MC75A4-3	700-013917-0000/ MC75A4-3-001	700-013670-0000	700-013670-0100
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
VSP 7400-48Y front-to-back	Y	—	—	—
VSP 7400-48Y back-to-front	—	Y	—	—
VSP 7400-48Y front-to-back DC	—	—	Y	—
VSP 7400-48Y back-to-front DC	—	—	—	Y

Table 18: XA1400 Series Power Supplies

Platform	12 V DC XA1400-PWR-ADPT
XA1440	Y
XA1480	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 more information, see Administering VOSS.

Layer 2

Table 19: Layer 2 Maximums

Attribute	Product	Maximum number supported
MAC table size (without SPBM)	5520 Series	81,920
	VSP 4450 Series	32,000
	VSP 4900 Series	80,000
	VSP 7200 Series	224,000
	VSP 7400 Series	160,000
	VSP 8000 Series	224,000
	XA1400 Series	2,000 for XA1440 4,000 for XA1480

Table continues…

Attribute	Product	Maximum number supported
MAC table size (with SPBM)	5520 Series	40,960
	VSP 4450 Series	16,000
	VSP 4900 Series	40,000
	VSP 7200 Series	112,000
	VSP 7400 Series	80,000
	VSP 8000 Series	112,000
	XA1400 Series	2,000 for XA1440 4,000 for XA1480
Endpoint Tracking MAC addresses per switch	5520 Series	8,000
	VSP 4450 Series	n/a
	VSP 4900 Series	n/a
	VSP 7200 Series	8,000
	VSP 7400 Series	8,000
	VSP 8000 Series	8,000
	XA1400 Series	n/a
Directed Broadcast interfaces	5520 Series	200 See Maximum Number of Directed Broadcast Interfaces on page 48.
	VSP 4450 Series	n/a
	VSP 4900 Series	200 See Maximum Number of Directed Broadcast Interfaces on page 48.
	VSP 7200 Series	200 See Maximum Number of Directed Broadcast Interfaces on page 48.
	VSP 7400 Series	200 See Maximum Number of Directed Broadcast Interfaces on page 48.
	VSP 8000 Series	200 See Maximum Number of Directed Broadcast Interfaces on page 48.

Table continues…

Attribute	Product	Maximum number supported
	XA1400 Series	n/a
Port-based VLANs **Note:** When you use Flex-UNI functionality, you can use the complete range from 1 to 4096 for port VLAN IDs.	5520 Series	4,059
	VSP 4450 Series	4,059
	VSP 4900 Series	4,059
	VSP 7200 Series	4,059
	VSP 7400 Series	4,059
	VSP 8000 Series	4,059
	XA1400 Series	500
Private VLANs	5520 Series	200
	VSP 4450 Series	200
	VSP 4900 Series	200
	VSP 7200 Series	200
	VSP 7400 Series	200
	VSP 8000 Series	VSP 8404C = 400 Other VSP 8000 Series platforms = 200
	XA1400 Series	n/a
Protocol-based VLANs (IPv6 only)	5520 Series	1
	VSP 4450 Series	1
	VSP 4900 Series	1
	VSP 7200 Series	1
	VSP 7400 Series	1
	VSP 8000 Series	1
	XA1400 Series	n/a
RSTP instances	5520 Series	1
	VSP 4450 Series	1
	VSP 4900 Series	1
	VSP 7200 Series	1
	VSP 7400 Series	1
	VSP 8000 Series	1
	XA1400 Series	1
MSTP instances	5520 Series	12
	VSP 4450 Series	12
	VSP 4900 Series	12
	VSP 7200 Series	12

Table continues…

Attribute	Product	Maximum number supported
	VSP 7400 Series	64
	VSP 8000 Series	12
	XA1400 Series	12
LACP aggregators	5520 Series	48-port models: up to 60 with channelization 24-port models: up to 36 with channelization
	VSP 4450 Series	24
	VSP 4900 Series	VSP4900-48P: 52 (48 fixed ports + 4 VIM ports) VSP4900-24S, VSP4900-24XE, VSP4900-12MXU-12XE : 28 (24 fixed + 4 VIM ports)
	VSP 7200 Series	54 (up to 72 with channelization)
	VSP 7400 Series	VSP 7432CQ = 32 (up to 125 with channelization) configured in Full Port mode VSP 7400-48Y = 56 configured in Full Port mode
	VSP 8000 Series	84 (up to 96 with channelization)
	XA1400 Series	8
Ports per LACP aggregator	5520 Series	8 active
	VSP 4450 Series	8 active
	VSP 4900 Series	8 active
	VSP 7200 Series	8 active
	VSP 7400 Series	8 active
	VSP 8000 Series	8 active
	XA1400 Series	8
MLT groups	5520 Series	48-port models: up to 60 with channelization

Table continues…

Attribute	Product	Maximum number supported
		24-port models: up to 36 with channelization
	VSP 4450 Series	50
	VSP 4900 Series	VSP4900-48P: 52 (48 fixed ports + 4 VIM ports) VSP4900-24S, VSP4900-24XE, VSP4900-12MXU-12XE : 28 (24 fixed + 4 VIM ports)
	VSP 7200 Series	54 (up to 72 with channelization)
	VSP 7400 Series	VSP 7432CQ = 32 (up to 125 with channelization) configured in Full Port mode VSP 7400-48Y = 56 configured in Full Port mode
	VSP 8000 Series	84 (up to 96 with channelization)
	XA1400 Series	8
Ports per MLT group	5520 Series	8 active
	VSP 4450 Series	8
	VSP 4900 Series	8
	VSP 7200 Series	8
	VSP 7400 Series	8
	VSP 8000 Series	8
	XA1400 Series	8
Link State Tracking (LST) groups	5520 Series	48
	VSP 4450 Series	48
	VSP 4900 Series	48
	VSP 7200 Series	48
	VSP 7400 Series	48
	VSP 8000 Series	48
	XA1400 Series	n/a

Table continues…

Attribute	Product	Maximum number supported
Interfaces per LST group	5520 Series	8 upstream 128 downstream
	VSP 4450 Series	8 upstream 128 downstream
	VSP 4900 Series	8 upstream 128 downstream
	VSP 7200 Series	8 upstream 128 downstream
	VSP 7400 Series	8 upstream 128 downstream
	VSP 8000 Series	8 upstream 128 downstream
	XA1400 Series	n/a
SLPP VLANs	5520 Series	128
	VSP 4450 Series	128
	VSP 4900 Series	128
	VSP 7200 Series	128
	VSP 7400 Series	500
	VSP 8000 Series	128
	XA1400 Series	128
VLACP interfaces	5520 Series	48-port models: up to 60 with channelization 24-port models: up to 36 with channelization
	VSP 4450 Series	50
	VSP 4900 Series	VSP4900-48P: 52 (48 fixed ports + 4 VIM ports) VSP4900-24S, VSP4900-24XE, VSP4900-12MXU-12XE : 28 (24 fixed + 4 VIM ports)
	VSP 7200 Series	54 (up to 72 with channelization)

Table continues…

Attribute	Product	Maximum number supported
	VSP 7400 Series	VSP 7432CQ = 32 (up to 125 with channelization) configured in Full Port mode VSP 7400-48Y = 56 configured in Full Port mode
	VSP 8000 Series	84 (up to 96 with channelization)
	XA1400 Series	8
Microsoft NLB cluster IP interfaces	5520 Series	200 See Maximum Number of Microsoft NLB Cluster IP Interfaces on page 48.
	VSP 4450 Series	n/a
	VSP 4900 Series	200 See Maximum Number of Microsoft NLB Cluster IP Interfaces on page 48.
	VSP 7200 Series	200 See Maximum Number of Microsoft NLB Cluster IP Interfaces on page 48.
	VSP 7400 Series	200 See Maximum Number of Microsoft NLB Cluster IP Interfaces on page 48.
	VSP 8000 Series	200 See Maximum Number of Microsoft NLB Cluster IP Interfaces on page 48.
	XA1400 Series	n/a

Maximum Number of Directed Broadcast Interfaces

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.

Maximum Number of Microsoft NLB Cluster IP Interfaces

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.

IP Unicast

Table 20: IP Unicast Maximums

Attribute	Product	Maximum number supported
IP interfaces (IPv4 or IPv6 or IPv4+IPv6)	5520 Series	500 See IP Unicast Maximums for 5520 Series and VSP 4900 Series on page 58.
	VSP 4450 Series	256
	VSP 4900 Series	500 See IP Unicast Maximums for 5520 Series and VSP 4900 Series on page 58.
	VSP 7200 Series	505 See IP Unicast Maximums for VSP 7200 Series, VSP 8200 Series, and VSP 8400 Series on page 59.
	VSP 7400 Series	1,000

Table continues…

Attribute	Product	Maximum number supported
		See IP Unicast Maximums for VSP 7400 Series on page 59.
	VSP 8000 Series	VSP 8404C = 500 Other VSP 8000 Series platforms = 505 See IP Unicast Maximums for VSP 7200 Series, VSP 8200 Series, and VSP 8400 Series on page 59.
	XA1400 Series	500 (IPv4 only)
VRRP interfaces (IPv4 or IPv6)	5520 Series	252 See IP Unicast Maximums for 5520 Series and VSP 4900 Series on page 58.
	VSP 4450 Series	64
	VSP 4900 Series	252 See IP Unicast Maximums for 5520 Series and VSP 4900 Series on page 58.
	VSP 7200 Series	252 See IP Unicast Maximums for VSP 7200 Series, VSP 8200 Series, and VSP 8400 Series on page 59.
	VSP 7400 Series	500 per switch 256 per VRF See IP Unicast Maximums for VSP 7400 Series on page 59.
	VSP 8000 Series	252 See IP Unicast Maximums for VSP 7200 Series, VSP 8200 Series, and VSP 8400 Series on page 59.
	XA1400 Series	64 (IPv4 only)
Routed Split Multi-Link Trunking (RSMLT) interfaces (IPv4 or IPv6 or IPv4+IPv6)	5520 Series	252
	VSP 4450 Series	252
	VSP 4900 Series	252

Table continues…

Attribute	Product	Maximum number supported
	VSP 7200 Series	252 See IP Unicast Maximums for VSP 7200 Series, VSP 8200 Series, and VSP 8400 Series on page 59.
	VSP 7400 Series	500 See IP Unicast Maximums for VSP 7400 Series on page 59.
	VSP 8000 Series	252 See IP Unicast Maximums for VSP 7200 Series, VSP 8200 Series, and VSP 8400 Series on page 59.
	XA1400 Series	n/a
VRRP interfaces with fast timers (200ms) - IPv4/IPv6	5520 Series	24
	VSP 4450 Series	24
	VSP 4900 Series	24
	VSP 7200 Series	24
	VSP 7400 Series	24
	VSP 8000 Series	24
	XA1400 Series	24
DvR Virtual IP interfaces	5520 Series	499 with vIST 500 without vIST
	VSP 4450 Series	501 with vIST 502 without vIST
	VSP 4900 Series	499 with vIST 500 without vIST
	VSP 7200 Series	501 with vIST 502 without vIST
	VSP 7400 Series	999 with vIST 1,000 without vIST
	VSP 8000 Series	VSP 8404C: • 499 with vIST • 500 without vIST

Table continues…

Attribute	Product	Maximum number supported
		Other VSP 8000 Series platforms: • 501 with vIST • 502 without vIST
	XA1400 Series	n/a
ECMP groups/paths per group	5520 Series	125/8 Overall limit: 1,000 ECMP paths
	VSP 4450 Series	500/4
	VSP 4900 Series	1,000/8
	VSP 7200 Series	1,000/8
	VSP 7400 Series	1,000/8
	VSP 8000 Series	1,000/8
	XA1400 Series	500/8
OSPF v2/v3 interfaces	5520 Series	100
	VSP 4450 Series	100
	VSP 4900 Series	500
	VSP 7200 Series	500
	VSP 7400 Series	500
	VSP 8000 Series	500
	XA1400 Series	48 (v2 only)
OSPF v2/v3 neighbors (adjacencies)	5520 Series	100
	VSP 4450 Series	100
	VSP 4900 Series	500
	VSP 7200 Series	500
	VSP 7400 Series	500
	VSP 8000 Series	500
	XA1400 Series	24 (v2 only)
OSPF areas	5520 Series	12 for each VRF 80 for the switch
	VSP 4450 Series	12 for each VRF 64 for the switch
	VSP 4900 Series	12 for each VRF 80 for the switch

Table continues…

Attribute	Product	Maximum number supported
	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
	XA1400 Series	12 for each VRF 64 for each switch
IPv4 ARP table	5520 Series	16,000
	VSP 4450 Series	6,000
	VSP 4900 Series	32,000 in non-SPB deployments 16,000 in SPB deployments
	VSP 7200 Series	48,000 in non-SPB deployments 32,000 in SPB deployments
	VSP 7400 Series	56,000 non-SPB deployments 40,000 SPB deployments
	VSP 8000 Series	48,000 in non-SPB deployments 32,000 in SPB deployments
	XA1400 Series	2,000 for XA1440 4,000 for XA1480
IPv4 CLIP interfaces	5520 Series	64
	VSP 4450 Series	64
	VSP 4900 Series	64
	VSP 7200 Series	64
	VSP 7400 Series	64
	VSP 8000 Series	64
	XA1400 Series	64
IPv4 RIP interfaces	5520 Series	100

Table continues…

Attribute	Product	Maximum number supported
	VSP 4450 Series	200
	VSP 4900 Series	200
	VSP 7200 Series	200
	VSP 7400 Series	200
	VSP 8000 Series	200
	XA1400 Series	200
IPv4 BGP peers	5520 Series	16
	VSP 4450 Series	12
	VSP 4900 Series	256
	VSP 7200 Series	256
	VSP 7400 Series	256
	VSP 8000 Series	256
	XA1400 Series	12
IPv4 VRFs with iBGP	5520 Series	16
	VSP 4450 Series	16
	VSP 4900 Series	16
	VSP 7200 Series	16
	VSP 7400 Series	16
	VSP 8000 Series	16
	XA1400 Series	n/a
IPv4/IPv6 VRF instances For additional information, see VRF Scaling on page 91.	5520 Series	258 including mgmt VRF and GRT
	VSP 4450 Series	128 including GRT
	VSP 4900 Series	258 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
	XA1400 Series	24 including GRT
IPv4 static ARP entries	5520 Series	2,000 for each VRF 10,000 for the switch
	VSP 4450 Series	200 for each VRF

Table continues…

Attribute	Product	Maximum number supported
		1,000 for the switch
	VSP 4900 Series	2,000 for each VRF 10,000 for the switch
	VSP 7200 Series	2,000 for each VRF 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
	XA1400 Series	200 for each VRF 1,000 for the switch
IPv4 static routes	5520 Series	1,000 for each VRF 5,000 for the switch
	VSP 4450 Series	1,000 for each VRF 1,000 for the switch
	VSP 4900 Series	1,000 for each VRF 5,000 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
	XA1400 Series	1,000 for each VRF 5,000 for the switch
IPv4 route policies	5520 Series	500 for each VRF 5,000 for the switch
	VSP 4450 Series	500 for each VRF 5,000 for the switch
	VSP 4900 Series	500 for each VRF 5,000 for the switch
	VSP 7200 Series	500 for each VRF 5,000 for the switch

Table continues…

Attribute	Product	Maximum number supported
	VSP 7400 Series	500 for each VRF 5,000 for the switch
	VSP 8000 Series	500 for each VRF 5,000 for the switch
	XA1400 Series	500 for each VRF 5,000 for the switch
IPv4 UDP forwarding entries	5520 Series	256
	VSP 4450 Series	128
	VSP 4900 Series	512
	VSP 7200 Series	512
	VSP 7400 Series	1,024
	VSP 8000 Series	512
	XA1400 Series	128
IPv4 DHCP Relay forwarding entries	5520 Series	512
	VSP 4450 Series	128
	VSP 4900 Series	2048
	VSP 7200 Series	2048
	VSP 7400 Series	2048
	VSP 8000 Series	2048
	XA1400 Series	128
IPv6 DHCP Snoop entries in Source Binding Table	5520 Series	1,024
	VSP 4450 Series	1,024
	VSP 4900 Series	1,024
	VSP 7200 Series	1,024
	VSP 7400 Series	1,024
	VSP 8000 Series	1,024
	XA1400 Series	n/a
IPv6 Neighbor table	5520 Series	16,000
	VSP 4450 Series	4,000
	VSP 4900 Series	8,000
	VSP 7200 Series	8,000
	VSP 7400 Series	32,000
	VSP 8000 Series	8,000
	XA1400 Series	n/a

Table continues…

Attribute	Product	Maximum number supported
IPv6 static entries in Source Binding Table	5520 Series	128 per VRF 512 per system
	VSP 4450 Series	256
	VSP 4900 Series	256
	VSP 7200 Series	256
	VSP 7400 Series	256
	VSP 8000 Series	256
	XA1400 Series	n/a
IPv6 static neighbor records	5520 Series	128 per VRF 512 per system
	VSP 4450 Series	128
	VSP 4900 Series	128 per VRF 512 per system
	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
	XA1400 Series	n/a
IPv6 CLIP interfaces	5520 Series	64
	VSP 4450 Series	64
	VSP 4900 Series	64
	VSP 7200 Series	64
	VSP 7400 Series	64
	VSP 8000 Series	64
	XA1400 Series	n/a
IPv6 static routes	5520 Series	1,000
	VSP 4450 Series	1,000
	VSP 4900 Series	1,000
	VSP 7200 Series	1,000
	VSP 7400 Series	1,000
	VSP 8000 Series	1,000
	XA1400 Series	n/a

Table continues…

Attribute	Product	Maximum number supported
IPv6 6in4 configured tunnels	5520 Series	64
	VSP 4450 Series	64
	VSP 4900 Series	64
	VSP 7200 Series	64
	VSP 7400 Series	64
	VSP 8000 Series	64
	XA1400 Series	n/a
IPv6 DHCP Relay forwarding	5520 Series	256 per switch 10 per VRF
	VSP 4450 Series	128
	VSP 4900 Series	512 per switch 10 per VRF
	VSP 7200 Series	512 per switch 10 per VRF
	VSP 7400 Series	512
	VSP 8000 Series	512
	XA1400 Series	n/a
IPv6 BGP peers	5520 Series	16 Up to 8,000 IPv6 prefixes for BGPv6 peering
	VSP 4450 Series	12 Up to 8,000 IPv6 prefixes for BGPv6 peering
	VSP 4900 Series	256 Up to 8,000 IPv6 prefixes for BGPv6 peering
	VSP 7200 Series	256 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
	XA1400 Series	n/a
IPv6 VRFs with iBGP	5520 Series	16

Table continues…

Attribute	Product	Maximum number supported
	VSP 4450 Series	16
	VSP 4900 Series	16
	VSP 7200 Series	16
	VSP 7400 Series	16
	VSP 8000 Series	16
	XA1400 Series	n/a
BFD VRF instances	5520 Series	16
	VSP 4450 Series	16
	VSP 4900 Series	16
	VSP 7200 Series	16
	VSP 7400 Series	16
	VSP 8000 Series	16
	XA1400 Series	n/a
BFD sessions per switch (IPv4/IPv6) with default values	5520 Series	16
	VSP 4450 Series	16
	VSP 4900 Series	16
	VSP 7200 Series	16
	VSP 7400 Series	16
	VSP 8000 Series	16
	XA1400 Series	n/a

IP Unicast Maximums for 5520 Series and VSP 4900 Series

The maximum number of IP interfaces for 5520 Series and VSP 4900 Series is based on the following formulas:

- If you disable the VRF scaling boot configuration flag:
  - = 500 – (# 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:
  - = 500 – (# of VRRP IPv4 interfaces) – (# of VRRP IPv6 interfaces) - (# of RSMLT interfaces) – 2 (if IP Shortcuts is enabled) – 3

IP Unicast Maximums for VSP 7200 Series, VSP 8200 Series, and VSP 8400 Series

The maximum number of IP interfaces for VSP 7200 Series, VSP 8200 Series, and VSP 8400 Series is based on the following formulas:

- If you disable the VRF scaling boot configuration flag:
  - = 505 – (# 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:
  - = 505 – (# of VRRP IPv4 interfaces) – (# of VRRP IPv6 interfaces) - (# of RSMLT interfaces) – 2 (if IP Shortcuts is enabled) – 3

IP Unicast Maximums for VSP 7400 Series

The maximum number of IP interfaces for VSP 7400 Series is based on the following formulas:

- 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

Layer 3 Route Table Size

Table 21: Layer 3 Route Table Size Maximums

Attribute	Maximum number supported
IPv4 RIP routes	See Route Scaling on page 60.
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 22: 5520 Series

URPF mode	IPv6 mode	5520 Series		
		IPv4	IPv6 (prefix less than 64)	IPv6 (prefix greater than 64)
No	No	15,500	7,750	n/a
No	Yes	7,500	3,500	2,000
Yes	No	7,500	3,750	n/a
Yes	Yes	3,500	1,750	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 (not a combination of both).

Table 23: VSP 4450 Series, VSP 4900 Series, VSP 7200 Series, and VSP 8000 Series

URPF mode	IPv6 mode	VSP 4450 Series			VSP 7200 Series, VSP 4900 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	2,000

Table continues…

URPF mode	IPv6 mode	VSP 4450 Series			VSP 7200 Series, VSP 4900 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

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 24: 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).

Table 25: XA1400 Series

IPv4 BGP routes (control plane only)	15,488
IPv4 OSFP routes	15,488
IPv4 RIP routes	15,488
IPv4 routes	15,488
IPv4 SPB Shortcut routes	15,488

IP Multicast

Table 26: IP Multicast Maximums

Attribute	Product	Maximum number supported
Combination of VLANs + number of IPv4 senders + IPv6 senders (non-SPBM mode)	5520 Series	8,192
	VSP 4450 Series	4,059
	VSP 4900 Series	8,192
	VSP 7200 Series	8,192
	VSP 7400 Series	8,192
	VSP 8000 Series	8,192
	XA1400 Series	n/a
Combination of Layer 2 VSNs + number of IPv4 senders + number of IPv6 senders (SPBM mode)	5520 Series	8,192
	VSP 4450 Series	4,059
	VSP 4900 Series	8,192
	VSP 7200 Series	8,192
	VSP 7400 Series	8,192
	VSP 8000 Series	8,192
	XA1400 Series	n/a
IGMP/MLD interfaces (IPv4/IPv6)	5520 Series	4,059
	VSP 4450 Series	4,059
	VSP 4900 Series	4,059
	VSP 7200 Series	4,059
	VSP 7400 Series	4,059
	VSP 8000 Series	4,059
	XA1400 Series	n/a
PIM interfaces (IPv4/IPv6)	5520 Series	128 Active
	VSP 4450 Series	128 Active
	VSP 4900 Series	128 Active
	VSP 7200 Series	128 Active
	VSP 7400 Series	128 Active
	VSP 8000 Series	128 Active
	XA1400 Series	n/a
PIM Neighbors (IPv4/IPv6) (GRT Only)	5520 Series	128
	VSP 4450 Series	128
	VSP 4900 Series	128

Table continues…

Attribute	Product	Maximum number supported
	VSP 7200 Series	128
	VSP 7400 Series	128
	VSP 8000 Series	128
	XA1400 Series	n/a
PIM-SSM static channels (IPv4/IPv6)	5520 Series	4,000
	VSP 4450 Series	512
	VSP 4900 Series	4,000
	VSP 7200 Series	4,000
	VSP 7400 Series	4,000
	VSP 8000 Series	4,000
	XA1400 Series	n/a
Multicast receivers/IGMP joins (IPv4/IPv6) (per switch)	5520 Series	6,000
	VSP 4450 Series	1,000
	VSP 4900 Series	6,000
	VSP 7200 Series	6,000
	VSP 7400 Series	6,000
	VSP 8000 Series	6,000
	XA1400 Series	n/a
Total multicast routes (S,G,V) (IPv4/IPv6) (per switch)	5520 Series	4,000
	VSP 4450 Series	1,000
	VSP 4900 Series	6,000
	VSP 7200 Series	6,000
	VSP 7400 Series	6,000
	VSP 8000 Series	6,000
	XA1400 Series	n/a
Total multicast routes (S,G,V) (IPv4) on an SPB-PIM Gateway configured switch	5520 Series	4,000
	VSP 4450 Series	1,000
	VSP 4900 Series	3,000
	VSP 7200 Series	3,000
	VSP 7400 Series	3,000
	VSP 8000 Series	3,000
	XA1400 Series	n/a
Static multicast routes (S,G,V) (IPv4/IPv6)	5520 Series	4,000
	VSP 4450 Series	512

Table continues…

Attribute	Product	Maximum number supported
	VSP 4900 Series	4,000
	VSP 7200 Series	4,000
	VSP 7400 Series	4,000
	VSP 8000 Series	4,000
	XA1400 Series	n/a
Multicast enabled Layer 2 VSN (IPv4)	5520 Series	2,000
	VSP 4450 Series	1,000
	VSP 4900 Series	2,000
	VSP 7200 Series	2,000
	VSP 7400 Series	2,000
	VSP 8000 Series	2,000
	XA1400 Series	n/a
Multicast enabled Layer 3 VSN (IPv4)	5520 Series	256 including mgmt VRF and GRT
	VSP 4450 Series	128 including mgmt VRF and GRT
	VSP 4900 Series	256 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
	XA1400 Series	n/a
SPB-PIM Gateway controller S,Gs (source announcements) with MSDP (IPv4)	5520 Series	6,000
	VSP 4450 Series	6,000
	VSP 4900 Series	6,000
	VSP 7200 Series	6,000
	VSP 7400 Series	6,000
	VSP 8000 Series	6,000
	XA1400 Series	n/a
SPB-PIM Gateway controllers per SPB fabric (IPv4)	5520 Series	5
	VSP 4450 Series	5
	VSP 4900 Series	5
	VSP 7200 Series	5

Table continues…

Attribute	Product	Maximum number supported
	VSP 7400 Series	5
	VSP 8000 Series	5
	XA1400 Series	n/a
SPB-PIM Gateway nodes per SPB fabric (IPv4)	5520 Series	64
	VSP 4450 Series	64
	VSP 4900 Series	64
	VSP 7200 Series	64
	VSP 7400 Series	64
	VSP 8000 Series	64
	XA1400 Series	n/a
SPB-PIM Gateway interfaces per BEB (IPv4)	5520 Series	64
	VSP 4450 Series	64
	VSP 4900 Series	64
	VSP 7200 Series	64
	VSP 7400 Series	64
	VSP 8000 Series	64
	XA1400 Series	n/a
PIM neighbors per SPB-PIM Gateway node (IPv4)	5520 Series	64
	VSP 4450 Series	64
	VSP 4900 Series	64
	VSP 7200 Series	64
	VSP 7400 Series	64
	VSP 8000 Series	64
	XA1400 Series	n/a

Distributed Virtual Routing (DvR)

Table 27: 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.		

Table continues…

Attribute	Product	Maximum number supported
• 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	5520 Series	499 with vIST 500 without vIST
	VSP 4450 Series	501 with vIST 502 without vIST
	VSP 4900 Series	499 with vIST 500 without vIST
	VSP 7200 Series	501 with vIST 502 without vIST
	VSP 7400 Series	999 with vIST 1,000 without vIST
	VSP 8000 Series	VSP 8404C = 499 with vIST 500 without vIST Other VSP 8000 Series platforms = 501 with vIST 502 without vIST
	XA1400 Series	n/a
DvR domains per SPB fabric	5520 Series	16
	VSP 4450 Series	16
	VSP 4900 Series	16
	VSP 7200 Series	16
	VSP 7400 Series	16
	VSP 8000 Series	16
	XA1400 Series	n/a
Controller nodes per DvR domain with default route inject flag enabled 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.	5520 Series	8
	VSP 4450 Series	n/a
	VSP 4900 Series	8
	VSP 7200 Series	8
	VSP 7400 Series	8
	VSP 8000 Series	8
	XA1400 Series	n/a
Leaf nodes per DvR domain	5520 Series	250

Table continues…

Attribute	Product	Maximum number supported
	VSP 4450 Series	250
	VSP 4900 Series	250
	VSP 7200 Series	250
	VSP 7400 Series	250
	VSP 8000 Series	250
	XA1400 Series	n/a
DvR enabled Layer 2 VSNs	5520 Series	501 with vIST 502 without vIST
	VSP 4450 Series	501 with vIST 502 without vIST
	VSP 4900 Series	501 with vIST 502 without vIST
	VSP 7200 Series	501 with vIST 502 without vIST
	VSP 7400 Series	999 with vIST 1,000 without vIST
	VSP 8000 Series	501 with vIST 502 without vIST
	XA1400 Series	n/a
DvR host route scaling per DvR domain (scaling number includes local as well as foreign hosts of the Layer 2 VSN that are members of the domain) If DvR Layer 2 VSNs span DvR domains, and all DvR Controllers have an IP interface on the Layer 2 VSNs, then the DvR host scaling is network-wide, as DvR Controllers will consume as many host routes as there are hosts across all DvR domains.	5520 Series	48,000
	VSP 4450 Series	6,000
	VSP 4900 Series	32,000
	VSP 7200 Series	32,000
	VSP 7400 Series	40,000
	VSP 8000 Series	32,000
	XA1400 Series	n/a

VXLAN Gateway

Table 28: VXLAN Gateway Maximums

Attribute	Product	Maximum number supported
MAC addresses in base interworking mode	5520 Series	n/a
	VSP 4450 Series	n/a
	VSP 4900 Series	n/a
	VSP 7200 Series	112,000
	VSP 7400 Series	80,000
	VSP 8000 Series	112,000
	XA1400 Series	n/a
MAC addresses in full interworking mode	5520 Series	n/a
	VSP 4450 Series	n/a
	VSP 4900 Series	n/a
	VSP 7200 Series	74,000
	VSP 7400 Series	50,000
	VSP 8000 Series	74,000
	XA1400 Series	n/a
VNI IDs per node	5520 Series	n/a
	VSP 4450 Series	n/a
	VSP 4900 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
	XA1400 Series	n/a
VTEP destinations per node or VTEP	5520 Series	n/a
	VSP 4450 Series	n/a
	VSP 4900 Series	n/a
	VSP 7200 Series	500
	VSP 7400 Series	500
	VSP 8000 Series	500
	XA1400 Series	n/a

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

Table 29: OVSDB protocol support for VXLAN Gateway Maximums

Attribute	Product	Maximum number supported
Maximum controllers to which a single VTEP switch can connect	5520 Series	n/a
	VSP 4450 Series	n/a
	VSP 4900 Series	n/a
	VSP 7200 Series	3
	VSP 7400 Series	3
	VSP 8000 Series	3
	XA1400 Series	n/a

Filters, QoS, and Security

Table 30: Filters, QoS, and Security Maximums

Attribute	Product	Maximum number supported
For more information, see Filter Scaling on page 71.		
Total IPv4 Ingress rules/ACEs (Port/VLAN/InVSN based, Security/QoS filters)	5520 Series	1,024 (512 security and 512 QoS)
	VSP 4450 Series	1,020
	VSP 4900 Series	1,536
	VSP 7200 Series	766
	VSP 7400 Series	1,536
	VSP 8000 Series	VSP 8404C = 3,070 Other VSP 8000 Series platforms = 766
	XA1400 Series	500
Total IPv4 Egress rules/ACEs (Port based, Security filters)	5520 Series	336 80 if you enable the ipv6-egress-filter boot configuration flag
	VSP 4450 Series	255 200 if you enable the ipv6-egress-filter boot configuration flag
	VSP 4900 Series	248

Table continues…

Attribute	Product	Maximum number supported
	VSP 7200 Series	248 200 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
	XA1400 Series	500
Total IPv6 Ingress rules/ACEs (Port/VLAN/InVSN based, Security filters)	5520 Series	512
	VSP 4450 Series	255
	VSP 4900 Series	1024
	VSP 7200 Series	256
	VSP 7400 Series	767
	VSP 8000 Series	VSP 8404 = 511 VSP 8404C = 2,047 Other VSP 8000 Series platforms = 256
	XA1400 Series	n/a
Total IPv6 egress rules/ACEs (Port based, Security filters)	5520 Series	256
	VSP 4450 Series	256
	VSP 4900 Series	256
	VSP 7200 Series	256
	VSP 7400 Series	511
	VSP 8000 Series	256
	XA1400 Series	n/a
EAP and NEAP (clients per port)	5520 Series	32 for EAP 8,192 for NEAP
	VSP 4450 Series	32 for EAP

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.		8,192 for NEAP
	VSP 4900 Series	32 for EAP 8,192 for NEAP
	VSP 7200 Series	32 for EAP 8,192 for NEAP
	VSP 7400 Series	32 for EAP 8,192 for NEAP
	VSP 8000 Series	32 for EAP 8,192 for NEAP
	XA1400 Series	n/a

Filter Scaling

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

5520 Series

The switch supports the following maximum limits:

- 512 non-IPv6 ingress ACLs (inPort, inVSN, or inVlan):
  - 512 ACLs with 1 security ACE each OR
  - 256 ACLs with 1 QoS ACE each OR
  - a combination based on the following rule:
    - `( (num ACLs + num security ACEs) <= 1024) && ((num ACLs + num QoS ACEs) <= 512)`

  This maximum implies a VLAN member count of 1 for inVlan ACLs
- 512 IPv6 ingress ACLs (inPort):
  - 512 ACLs with 1 security ACE each OR
  - a combination based on the following rule:
    - `(num ACLs + num security ACEs) <= 512`
- 124 egress ACLs (outPort only):
  - 124 ACLs with 1 security ACE each (one of these ACLs can have 2 ACEs) OR
  - a combination based on the following rule:
    - `(num ACLs + num ACEs) <= 248`

  This maximum implies a port member count of 1 for outPort ACLs.
- 1534 ingress ACEs:

Theoretical maximum of 1534 implies 1 ingress ACL with 1023 security ACEs and 511 QoS ACEs

- Ingress ACEs supported: `(1024 (security) - # of ACLs) + (512 (QoS) - # of ACLs).`

This maximum also implies a VLAN member count of 1 for an inVlan ACL.

- 247 egress ACEs:

  Theoretical maximum of 247 implies 1 egress ACL with 247 security ACEs

  - Egress ACEs supported: `248 - # of ACLs.`

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

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 4900 Series

The switch supports the following maximum limits:

- 512 non-IPv6 ingress ACLs (inPort, inVSN, or inVlan):
  - 512 ACLs with 1 security ACE each OR
  - 256 ACLs with 1 QoS ACE each OR
  - a combination based on the following rule:
    - `( (num ACLs + num security ACEs) <= 1024) && ((num ACLs + num QoS ACEs) <= 512)`

  This maximum implies a VLAN member count of 1 for inVlan ACLs

- 512 IPv6 ingress ACLs (inPort):
  - 512 ACLs with 1 security ACE each OR
  - a combination based on the following rule:
    - `(num ACLs + num security ACEs) <= 512`
- 124 egress ACLs (outPort only):
  - 124 ACLs with 1 security ACE each (one of these ACLs can have 2 ACEs) OR
  - a combination based on the following rule:
    - `(num ACLs + num ACEs) <= 248`

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

- 1534 ingress ACEs:

  Theoretical maximum of 1534 implies 1 ingress ACL with 1023 security ACEs and 511 QoS ACEs

  - Ingress ACEs supported: `(1024 (security) - # of ACLs) + (512 (QoS) - # of ACLs).`

  This maximum also implies a VLAN member count of 1 for an inVlan ACL.

- 247 egress ACEs:

  Theoretical maximum of 247 implies 1 egress ACL with 247 security ACEs

  - Egress ACEs supported: `248 - # of ACLs.`

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

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 non-IPv6 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

- 256 IPv6 ingress ACLs (inPort,):
  - 256 ACLs with 1 security ACE each OR
  - 256 ACLs with 1 QoS ACE each OR
  - a combination based on the following rule:
    - `(num ACLs + num security ACEs) <= 256`
- 124 egress ACLs (outPort only):
  - 124 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)`

XA1400 Series

The switch supports the following maximum limits:

- 500 IPv4 ingress ACLs
- 500 IPv4 egress ACLs
- 500 IPv4 ingress ACEs
- 500 IPv4 egress ACEs

OAM and Diagnostics

Table 31: OAM and Diagnostics Maximums

Attribute	Product	Maximum number supported
EDM sessions	5520 Series	5
	VSP 4450 Series	5
	VSP 4900 Series	5
	VSP 7200 Series	5
	VSP 7400 Series	5
	VSP 8000 Series	5
	XA1400 Series	5
FTP sessions (IPv4/IPv6)	5520 Series	8 total (4 for IPv4 and 4 for IPv6)
	VSP 4450 Series	8 total (4 for IPv4 and 4 for IPv6)
	VSP 4900 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)
	XA1400 Series	4 (IPv4 only)
SSH sessions (IPv4/IPv6)	5520 Series	8 total (any combination of IPv4 and IPv6)
	VSP 4450 Series	8 total (any combination of IPv4 and IPv6)
	VSP 4900 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)
	XA1400 Series	8 (IPv4 only)

Table continues…

Attribute	Product	Maximum number supported
Telnet sessions (IPv4/IPv6)	5520 Series	16 total (8 for IPv4 and 8 for IPv6)
	VSP 4450 Series	16 total (8 for IPv4 and 8 for IPv6)
	VSP 4900 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)
	XA1400 Series	8 (IPv4 only)
TFTP sessions (IPv4/IPv6)	5520 Series	2 total (any combination of IPv4 and IPv6)
	VSP 4450 Series	2 total (any combination of IPv4 and IPv6)
	VSP 4900 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)
	VSP 8000 Series	2 total (any combination of IPv4 and IPv6)
	XA1400 Series	n/a
Mirrored ports (source)	5520 Series	48-port models: 47 (up to 58 with channelization) 24-port models: 23 (up to 34 with channelization)
	VSP 4450 Series	49
	VSP 4900 Series	51 (52 ports per chassis, 48 fixed ports plus up to 4 ports on the VIMs)
	VSP 7200 Series	53 (up to 71 with channelization)
	VSP 7400 Series	31 (up to 125 with channelization) with Advanced Feature Bandwidth Reservation

Table continues…

Attribute	Product	Maximum number supported
		configured in Full Port mode
	VSP 8000 Series	83 (up to 95 with channelization)
	XA1400 Series	7
Mirroring ports (destination)	5520 Series	4
	VSP 4450 Series	4
	VSP 4900 Series	4
	VSP 7200 Series	4
	VSP 7400 Series	4
	VSP 8000 Series	4
	XA1400 Series	4
Fabric RSPAN Port mirror instances per switch (Ingress only)	5520 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 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 4900 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

Table continues…

Attribute	Product	Maximum number supported
		Mirror. Only one I-SID offset for Egress Mirror.
	XA1400 Series	n/a
Fabric RSPAN Flow mirror instances per switch (Ingress only)	5520 Series	Filter ACL ACE sessions can be mapped to 24 unique I-SID offsets.
	VSP 4450 Series	Filter ACL ACE sessions can be mapped to only 1 mirror I-SID offset.
	VSP 4900 Series	Filter ACL ACE sessions can be mapped to 24 unique I-SID offsets.
	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.
	XA1400 Series	n/a
Fabric RSPAN Monitoring I-SIDs (network value)	5520 Series	1,000 Monitoring I-SIDs across SPB network
	VSP 4450 Series	1,000 Monitoring I-SIDs across SPB network
	VSP 4900 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
	XA1400 Series	n/a
sFlow sampling limit	5520 Series	3,100 samples per second
	VSP 4450 Series	125 samples per second
	VSP 4900 Series	3,100 samples per second
	VSP 7200 Series	3,100 samples per second
	VSP 7400 Series	9,000 samples per second

Table continues…

Attribute	Product	Maximum number supported
	VSP 8000 Series	3,100 samples per second
	XA1400 Series	n/a
IPFIX flows	5520 Series	36,863
	VSP 4450 Series	n/a
	VSP 4900 Series	n/a
	VSP 7200 Series	n/a
	VSP 7400 Series	32,767
	VSP 8000 Series	n/a
	XA1400 Series	n/a
Application Telemetry host monitoring - maximum number of monitored hosts **Note:** These resources are shared with the IPv4 Filter Ingress rules/ACEs.	5520 Series	382 hosts
	VSP 4450 Series	509 hosts
	VSP 4900 Series	382 hosts
	VSP 7200 Series	382 hosts
	VSP 7400 Series	767 hosts
	VSP 8000 Series	VSP 8404C = 1,534 hosts Other VSP 8000 Series platforms = 382 hosts
	XA1400 Series	n/a

Virtualization Scaling

Note:

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

- 5520 Series
- VSP 4450 Series
- VSP 7200 Series
- VSP 8200 Series
- VSP 8400 Series
- XA1400 Series

Table 32: Virtualization Maximums

Attribute	Product	Maximum number supported
Simultaneous Virtual Machines	VSP 4900 Series	Not supported
	VSP 7400 Series	6
CPU cores available to VMs	VSP 4900 Series	2
	VSP 7400 Series	6
Memory available to VMs	VSP 4900 Series	4 GB
	VSP 7400 Series	12 GB
Storage available to VMs	VSP 4900 Series	104 GB of 120 modular SSD
	VSP 7400 Series	100 GB
Total SRIOV vports available to VMs	VSP 4900 Series	16
	VSP 7400 Series	16
Vports available to single VM	VSP 4900 Series	16
	VSP 7400 Series	16

Fabric Scaling

This section lists the fabric scaling information.

Table 33: Fabric Maximums

Attribute	Product	Maximum number supported (with and without vIST)
Number of SPB regions	5520 Series	1
	VSP 4450 Series	1
	VSP 4900 Series	1
	VSP 7200 Series	1
	VSP 7400 Series	1
	VSP 8000 Series	1
	XA1400 Series	1
Number of B-VIDs	5520 Series	2
	VSP 4450 Series	2
	VSP 4900 Series	2
	VSP 7200 Series	2

Table continues…

Attribute	Product	Maximum number supported (with and without vIST)
	VSP 7400 Series	2
	VSP 8000 Series	2
	XA1400 Series	2
Maximum number of Physical and Logical (Fabric Extend) NNI interfaces/adjacencies	5520 Series	128
	VSP 4450 Series	255
	VSP 4900 Series	255
	VSP 7200 Series	255
	VSP 7400 Series	255
	VSP 8000 Series	255
	XA1400 Series	255 without IPsec 64 with IPsec
SPBM enabled nodes per area (BEB + BCB)	5520 Series	800
	VSP 4450 Series	550
	VSP 4900 Series	800
	VSP 7200 Series	800
	VSP 7400 Series	2,000
	VSP 8000 Series	800
	XA1400 Series	550
Number of BEBs this node can share services with (Layer 2 VSNs, Layer 3 VSNs, E-Tree, Multicast, Transparent Port UNI). **Note:** vIST clusters are counted as 3 nodes. Each Fabric Extend IS-IS adjacency or VXLAN remote VTEP reduces this number by 1.	5520 Series	2,000
	VSP 4450 Series	500
	VSP 4900 Series	500
	VSP 7200 Series	500
	VSP 7400 Series	2,000
	VSP 8000 Series	500
	XA1400 Series	n/a
Maximum number of vIST/IST clusters this node can share I-SIDs with	5520 Series	2,000
	VSP 4450 Series	500
	VSP 4900 Series	330
	VSP 7200 Series	330
	VSP 7400 Series	2,000
	VSP 8000 Series	330
	XA1400 Series	n/a
Layer 2 MAC table size (with SPBM)	5520 Series	40,000

Table continues…

Attribute	Product	Maximum number supported (with and without vIST)
	VSP 4450 Series	16,000
	VSP 4900 Series	40,000
	VSP 7200 Series	112,000
	VSP 7400 Series	80,000
	VSP 8000 Series	112,000
	XA1400 Series	2,000 for XA1440 4,000 for XA1480
I-SIDs supported	5520 Series	See Number of I-SIDs supported on page 88
	VSP 4450 Series	See Number of I-SIDs supported on page 88
	VSP 4900 Series	See Number of I-SIDs supported on page 88
	VSP 7200 Series	See Number of I-SIDs supported on page 88
	VSP 7400 Series	See Number of I-SIDs supported on page 88
	VSP 8000 Series	See Number of I-SIDs supported on page 88
	XA1400 Series	See Number of I-SIDs supported on page 88
Maximum number of Layer 2 VSNs per switch	5520 Series	3,580
	VSP 4450 Series	1,000
	VSP 4900 Series	4,059
	VSP 7200 Series	4,059
	VSP 7400 Series	4,000
	VSP 8000 Series	4,059
	XA1400 Series	124
Maximum number of Switched UNI I-SIDs per switch	5520 Series	See Number of I-SIDs supported on page 88
	VSP 4450 Series	See Number of I-SIDs supported on page 88
	VSP 4900 Series	See Number of I-SIDs supported on page 88
	VSP 7200 Series	See Number of I-SIDs supported on page 88

Table continues…

Attribute	Product	Maximum number supported (with and without vIST)
	VSP 7400 Series	See Number of I-SIDs supported on page 88
	VSP 8000 Series	See Number of I-SIDs supported on page 88
	XA1400 Series	n/a
Maximum number of Transparent Port UNIs per switch	5520 Series	48-port models: 48 24-port models: 24
	VSP 4450 Series	48
	VSP 4900 Series	52
	VSP 7200 Series	54 (up to 72 with channelization)
	VSP 7400 Series	VSP 7432CQ = 32 (up to 125 with channelization) configured in Full Port mode VSP 7400-48Y = 56 configured in Full Port mode
	VSP 8000 Series	84 (up to 96 with channelization)
	XA1400 Series	n/a
Maximum number of E-Tree PVLAN UNIs per switch	5520 Series	200
	VSP 4450 Series	200
	VSP 4900 Series	200
	VSP 7200 Series	200
	VSP 7400 Series	200
	VSP 8000 Series	VSP 8404C = 400 Other VSP 8000 Series platforms = 200
	XA1400 Series	n/a
Maximum number of Layer 3 VSNs per switch See VRF Scaling on page 91.	5520 Series	256 including mgmt VRF and GRT
	VSP 4450 Series	128 including mgmt VRF and GRT
	VSP 4900 Series	256 including mgmt VRF and GRT

Table continues…

Attribute	Product	Maximum number supported (with and without vIST)
	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
	XA1400 Series	23
Maximum number of SPB Layer 2 multicast UNI I-SIDs	5520 Series	See Number of I-SIDs supported on page 88
	VSP 4450 Series	See Number of I-SIDs supported on page 88
	VSP 4900 Series	See Number of I-SIDs supported on page 88
	VSP 7200 Series	See Number of I-SIDs supported on page 88
	VSP 7400 Series	See Number of I-SIDs supported on page 88
	VSP 8000 Series	See Number of I-SIDs supported on page 88
	XA1400 Series	n/a
Maximum number of SPB Layer 3 multicast UNI I-SIDs	5520 Series	Maximum 4,000 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 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 4900 Series	Maximum 6,000 for a BEB: Due to internal resource sharing IP Multicast scaling depends on network topology. Switch will issue

Table continues…

Attribute	Product	Maximum number supported (with and without vIST)
		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.
	XA1400 Series	n/a
Maximum number of FA ISID/VLAN assignments per port	5520 Series	94
	VSP 4450 Series	94
	VSP 4900 Series	94
	VSP 7200 Series	94
	VSP 7400 Series	94
	VSP 8000 Series	94
	XA1400 Series	n/a
Maximum number of IP multicast S,Gs when operating as a BCB	5520 Series	16,000
	VSP 4450 Series	1,000
	VSP 4900 Series	16,000
	VSP 7200 Series	16,000
	VSP 7400 Series	50,000

Table continues…

Attribute	Product	Maximum number supported (with and without vIST)
	VSP 8000 Series	16,000
	XA1400 Series	2,000

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	5520 Series	4,000	4,000
	VSP 4450 Series	1,000	1,000
	VSP 4900 Series	4,000	4,000
	VSP 7200 Series	4,000	4,000
	VSP 7400 Series	4,000	4,000
	VSP 8000 Series	4,000	4,000
	XA1400 Series	n/a	150
6	5520 Series	3,500	4,000
	VSP 4450 Series	1,000	1,000
	VSP 4900 Series	3,500	4,000
	VSP 7200 Series	3,500	4,000
	VSP 7400 Series	3,500	4,000
	VSP 8000 Series	3,500	4,000
	XA1400 Series	n/a	150
10	5520 Series	2,900	4,000
	VSP 4450 Series	650	1,000
	VSP 4900 Series	2,900	4,000
	VSP 7200 Series	2,900	4,000
	VSP 7400 Series	2,900	4,000
	VSP 8000 Series	2,900	4,000
	XA1400 Series	n/a	150
20	5520 Series	2,000	4,000
	VSP 4450 Series	350	700

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 4900 Series	2,000	4,000
	VSP 7200 Series	2,000	4,000
	VSP 7400 Series	2,000	4,000
	VSP 8000 Series	2,000	4,000
	XA1400 Series	n/a	150
48	5520 Series	1,000	2,000
	VSP 4450 Series	n/a	n/a
	VSP 4900 Series	1,000	2,000
	VSP 7200 Series	1,000	2,000
	VSP 7400 Series	1,000	2,000
	VSP 8000 Series	1,000	2,000
	XA1400 Series	n/a	150
72	5520 Series	750	1,500
	VSP 4450 Series	n/a	n/a
	VSP 4900 Series	750	1,500
	VSP 7200 Series	750	1,500
	VSP 7400 Series	750	1,500
	VSP 8000 Series	750	1,500
	XA1400 Series	n/a	150
100	5520 Series	550	1,100
	VSP 4450 Series	n/a	n/a
	VSP 4900 Series	550	1,100
	VSP 7200 Series	550	1,100
	VSP 7400 Series	550	1,100
	VSP 8000 Series	550	1,100
	XA1400 Series	n/a	150
128	5520 Series	450	900
	VSP 4450 Series	n/a	n/a
	VSP 4900 Series	450	900
	VSP 7200 Series	450	900
	VSP 7400 Series	450	900
	VSP 8000 Series	450	900
	XA1400 Series	n/a	150
250	5520 Series	n/a	n/a

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 4450 Series	n/a	n/a
	VSP 4900 Series	240	480
	VSP 7200 Series	240	480
	VSP 7400 Series	240	480
	VSP 8000 Series	240	480
	XA1400 Series	n/a	150

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 Series 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 might 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 Series releases prior to 4.1.0.0 might 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 might 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.

5520 Series, VSP 4900 Series, 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 might 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. When VRF scaling is disabled, you can have a maximum of 24 VRFs.

Chapter 6: Important Notices

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

ExtremeCloud IQ Support for VSP Series

ExtremeCloud IQ provides cloud-managed networking, and delivers unified, full-stack management of wireless access points, switches, and routers. It enables onboarding, configuration, monitoring, troubleshooting, reporting, and more. Using innovative machine learning and artificial intelligence technologies, ExtremeCloud IQ analyzes and interprets millions of network and user data points, from the network edge to the data center, to power actionable business and IT insights, and to deliver new levels of network automation and intelligence.

ExtremeCloud IQ supports the following platforms:

- VSP4900-48P
- VSP 7400 Series
- XA1400 Series
- 5520 Series

For the most current information on switches supported by ExtremeCloud™ IQ, see ExtremeCloud™ IQ Learning What's New.

VOSS supports a zero touch connection to ExtremeCloud IQ. Zero touch deployment is used to deploy and configure a switch using ExtremeCloud IQ.

VOSS integrates with ExtremeCloud IQ using IQAgent. When you enable IQAgent, you can configure and monitor VOSS devices using ExtremeCloud IQ.

For more information, see:

- Configuring User Interfaces and Operating Systems for VOSS
- Troubleshooting VOSS

For more information about ExtremeCloud IQ, go to https://www.extremenetworks.com/support/documentation/extremecloud-iq/.

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.

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.

Base MAC Address Assignment for 5520 Switches

When running ExtremeXOS, the 5520 switch uses a base MAC address at offset 0 for both the default management port and in-band VLAN utilizing DHCP, for example, 00:c0:cc:8b:68:00. When the switch runs VOSS, it uses a base MAC at offset 0x81 for the default management port (for example, 00:c0:cc:8b:68:81) and offset 256 for the in-band VLAN (for example, 00:c0:cc:8b:69:00).

Note:
The address assignment for the in-band VLAN assumes that the VLAN has a mac-offset value of 0 assigned. If a different mac-offset value is assigned, the MAC address changes accordingly. For example, if mac-offset is 10, then the associated MAC address is 00:c0:cc:8b:69:0A.

When using a DHCP client on the switch, the switch sends a common DHCP client identifier equal to the base MAC address of the switch that is printed on the switch label. Because of this, assuming a standard DHCP pool configuration, the DHCP server always recognizes the switch by the same IP address, regardless of whether EXOS or VOSS is running on the switch.

If you want to statically assign IP addresses on the DHCP server, assign them based upon the DHCP client ID. This will ensure that the bindings do not change when the switch alternates between EXOS and VOSS. If you assign the DHCP IP addresses based on MAC addresses, you will need to configure multiple entries – one for the 0 offset and one for the 0x81 offset – to account for the different ways in which the two operating systems assign base MAC addresses.

Feature-Based Licensing

The following VOSS platforms support a licensing model that includes Base and Premier licenses:

- VSP 4450 Series
- VSP 4900 Series
- VSP 7200 Series
- VSP 7400 Series
- VSP 8200 Series
- VSP 8400 Series

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	• DvR Controller • DvR interfaces on more than 24 VRFs/Layer 3 VSNs on Leaf nodes **Note:** DvR Leaf functionality is part of the base software license and the software allows you to create DvR interfaces on Layer 3 VSNs on Leaf nodes. Because a Premier license is required to configure more than 24 VRFs, for deployments where DvR Controllers have more than 24 VRFs configured with DvR, then Leaf nodes only create the first 24 Layer 3 VSNs (VRFs) and no more, unless you install a Premier or Premier with MACsec license. • Extreme Integrated Application Hosting (does not apply to VSP 5520 Series) • Fabric Connect Layer 3 Virtual Services Networks (VSNs) • Greater than 16 BGP peers • Greater than 24 VRFs • VXLAN Gateway
Premier with MACsec License	All features in Premier license, plus: • IEEE 802.1AE MACsec

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

Licensing for Universal Hardware (5520 Series)

In VOSS 8.2.5, the following topics apply to Extreme Networks 5520 Series hardware. Because the 5520 Series hardware supports more than one Network Operating System (NOS) personality, it uses a licensing scheme that is NOS agnostic.

Feature Licensing for Universal Hardware

Note:

The information in this section applies only to ExtremeSwitching 5520 Series hardware.

Extreme Networks offers universal hardware products that support more than one Network Operating System (NOS) personality. The universal hardware products share a unified license, which is NOS agnostic.

The Base License, which is included with the purchase of the switch, enables the basic networking capabilities of the device. You can purchase additional licenses separately to enable advanced features on the switch.

Licenses are tied to the switch serial number. After you generate the license through the Extreme Networks Support Portal at https://extremeportal.force.com/ExtrLicenseLanding, you can install the license on the switch manually. In future VOSS releases, you will be able to use ExtremeCloud IQ to obtain licenses for universal hardware switches.

The following sections detail the different categories of licenses.

Evaluation License

New ExtremeSwitching 5520 Series switches include a factory-default (Evaluation) license that enables the use of all features, except MACsec, for a duration of 30 days. You can configure all features without restrictions and save the configuration.

You cannot configure new features after the 30-day period, but the switch continues to run with the existing configured features. If you reboot the switch after the 30-day period, and a valid software license is not present, licensed features in the configuration are not loaded. You must install a valid license to enable licensed features.

Base License

A Base license gives customers the right to use Base software features on the switch.

Licenses for Advanced Features

Licenses enable advanced features not available in the Base License. The following table provides information on the features enabled by each license, if the hardware supports the feature. For information on supported features, see VOSS Feature Support Matrix.

License type	Supported features
MACsec License	IEEE 802.1AE MACsec
Premier License	• DvR Controller • Fabric Connect Layer 3 Virtual Services Networks (VSNs) • Greater than four OSPF active Interfaces • Greater than two BGP peers • Greater than 24 VRFs

License Types and Part Numbers

The following table lists the license types and the associated part numbers.

License Type	Part Number / Order Code
MACsec License for 5520 Series	5000-MACSEC-LIC
Premier License for 5520 Series	5000-PRMR-LIC

ExtremeCloud™ IQ Pilot License

ExtremeSwitching 5520 Series switches include a one-year subscription to an ExtremeCloud™ IQ Pilot license.

Note:
The entitlement period starts the day the switch ships from Extreme Networks or an Extreme Networks distribution partner.

ExtremeCloud IQ enables end-to-end network management and operations, delivering a fully integrated, extensible platform that simplifies the design, deployment, and security of networks from the edge to the data center, while simultaneously unlocking valuable IT and business insights. To activate these premium Pilot level capabilities, go to https://www.extremenetworks.com/universalswitch-xiq-pilot.

Install and Uninstall Licenses on Universal Switches

This topic explains how to obtain, activate, and transfer licenses on universal hardware switches.

Obtain and Install a License

In future VOSS releases, in addition to the CLI method explained below, you will be able to use ExtremeCloud IQ to obtain licenses for universal hardware switches. ExtremeCloud IQ allows you to bulk license multiple devices. For information about using ExtremeCloud IQ, go to https://www.extremenetworks.com/extremecloud-iq/.

To obtain and install a license, follow these steps:

Note:
You should have received by email a license voucher after your purchase of a switch. You will need the voucher ID number on this email to generate a license.

1. Upon delivery, the switch has pre-GA (general availability) software installed. Upgrade the switch so that it is running the GA version of VOSS 8.2.5.0.

   To download the latest GA software, visit the Extreme Networks Support portal.
2. To obtain a license file, go to the Extreme Networks Support portal and do the following:
   a. Select **Assets** > **Licenses Home**.
   b. Select **Generate License**.
   c. In the **Generate License** pop-up window, type the ID number in the Voucher ID box and then select **Next**.
   d. Type the hardware serial number of the switch to which the license will be applied.
   e. Check the box to acknowledge the Terms and Conditions and then select **Submit**.
   f. Locate the license file at the bottom of the Voucher Details page.
3. Download the license file onto the switch.
4. Install the license, using the command `load-license` *license_filename*.

VOSS verifies the license and activates the features that correspond to the license category (MACsec or Premier).

For more information, see either of the following:

CLI	"License Installation using CLI" in *Administering VOSS* for VOSS 8.2.
EDM	"License Installation using EDM" in *Administering VOSS* for VOSS 8.2.

Display License Information

To display the license level installed on your switch, issue the command `show license`.

Transfer a License

You can permanently remove a license, which allows you to transfer the license to another switch. This should only be done when preparing to return a defective switch for a replacement switch (RMA).

To uninstall a license permanently from a universal hardware switch, use the command: `no license macsec` or `no license premier`.

The `no license` command invalidates the feature license and generates a revocation certificate, which is the first step to releasing the license entitlement back to the license entitlement manager (LEM). The revocation certificate is contained in a file where the first part of the file name is the switch serial number and the file extension is `.rvk`.

To transfer a license from a defective switch to a replacement switch (RMA), follow these steps.

1. Go to the Extreme Networks Support portal.
2. Select **Assets** > **Licenses Home**.
3. Select **License Transfer**.
4. Enter the defective unit's serial number, the replacement unit's serial number, and the RMA/case number.
5. Generate the new license, following the process in step 2 in Obtain and Install a License on page 97.
6. Download the license file onto the switch.
7. Install the license, using the command `load-license` *license_filename*.

Subscription Licensing for XA1400 Series

Each XA1400 Series device requires a subscription license.

Licenses are tied to the switch Base MAC address and switch model type. After you generate the license through Extreme Networks Support Portal at https://extremeportal.force.com/ExtrLicenseLanding, you can install the license on the switch.

Note:

VOSS Release 8.0.50 or later is required to support subscription licenses generated through the Extreme Networks Support Portal.

The following sections detail the different categories of licenses supported on the XA1400 Series switch.

Factory Default Trial License

A new switch includes a 60-day Factory Default Trial License starting from the time the switch is first booted. You can configure all features (except MACsec), without restrictions and save the configuration. No license file is required.

The system generates warning messages to inform you about the time remaining in the license period. The alerts appear once every 5 days for the first 55 days, and then once daily for the last 5

days. If you reboot the switch after the 60-day period, and a valid software license is not present, the licensed features in the configuration are not loaded. You must install a valid license to enable the licensed features.

Subscription License

All subscription licenses support all VOSS features on the switch, plus software upgrades and technical support services entitlement during the license term. A one, three, or five year subscription license is required for each XA1400 Series device. Three services entitlement tiers of license are available: ExtremeWorks, PartnerWorks, and ExtremeWorks Premier.

A Subscription License is available in two bandwidth tiers of licenses: Small License and Medium License. A Small License enables up to 100 Mbps aggregate throughput Fabric Extend WAN tunneling connectivity, and a Medium License enables up to 500 Mbps aggregate throughput Fabric Extend WAN tunneling connectivity.

License expiry notifications are sent to the console and management station every 30 days until the last 30 days of the subscription. Then every 5 days until the last 9 days of the subscription, and then daily until the Subscription License expires.

When a subscription expires, notification messages are shown on the console and in the alarms database, indicating that the license is expired. Existing software functionality is not impaired upon subscription license expiry. However, software upgrades are disallowed until the new license is activated. Additionally, access to Software and Services GTAC support is suspended for the product until a valid license is activated.

Supported Browsers

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

- Microsoft Edge 79.0.309.71 (released in January 2020)
- Microsoft Internet Explorer 11.+
- Mozilla Firefox 72+
- Google Chrome 80+
- Safari 13+

For optimal performance, use Mozilla Firefox or Google Chrome.

MLT Configuration

The following considerations apply when you configure link aggregation into your network using VOSS 8.2.5.

Before creating and configuring an MLT, refer to the following guidelines to understand the commands for adding VLANs to an LACP-enabled MLT. It is important to use the correct commands to avoid LACP churn.

- If only one port is part of the MLT/LAG, use the command `vlan members add` *<1-4059>* `{slot/port[/sub-port][-slot/port[/sub-port]] [,...]}` to add newer VLANs to the LAG.
- If two or more ports with several VLANs are active members of the MLT/LAG, you must use the command `mlt` *<1-512>* `vlan` *<1-4059>* to add new VLANs.
- If at least one port is active on the MLT/LAG (LACP), and you need to add a second port that is physically up and has the same key, you must use the command `mlt` *<1-512>* `vlan` *<1-4059>*. The port values must match. If the port values do not match, the new port enters the churn condition.
- If the switch displays a persistent error saying that you cannot change the port VLAN membership, you must correct the configuration during a maintenance window:
  1. Shut down the ports.
  2. Disable LACP on the ports.
  3. Add all VLANs to the port members being aggregated.
  4. Enable LACP on the ports.
  5. Enable the ports.

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 Series.

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.

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 with 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.

For information about feature support across all VOSS platforms, see VOSS Feature Support Matrix.

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 8.2.5

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 could 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-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 could 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 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.	Use a v3 interface as querier in a LAN segment that has snoop-enabled v2 and v3 interfaces.

Table continues…

Issue number	Description	Workaround
	• 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 re-enable 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 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	Reconfigure the 4 byte AS confederation identifier and peers on the device, and reboot.

Table continues…

Issue number	Description	Workaround
	a reboot. This problem occurs when 4 Byte AS is enabled with confederation.	
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 system displays the following message: `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 need to meet. The actual minimum password requirements you need to meet are configured on your system by the administrator.	None.
VOSS-1367	The configuration file always includes the router ospf entry 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 log in 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.
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.

Table continues…

Issue number	Description	Workaround
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-1403	EDM displays the user name as Admin, even though you log in using a different user name.	None.
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 RADIUS-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 one time.	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-1463 VOSS-1471	When you use Fabric Extend over IP (FE-IP) and Fabric Extend over Layer 2 VLAN (FE-VID) solution, if you change the ingress and egress .1p map, packets cannot follow correct internal QoS queues for FE tunnel to FE tunnel, or FE tunnel to regular NNI traffic.	Do not change the default ingress and egress .1p maps when using Fabric 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	None.

Table continues…

Issue number	Description	Workaround
	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.	
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-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.

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`
		Disable the alternate path.

Table continues…

Issue number	Description	Workaround
	`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`	
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 system displays the following error: `Error: Invalid IP Address or Hostname for SMTP server`	None.
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.`**

Table continues…

Issue number	Description	Workaround
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-2411	On a VSP 4450GSX-DC, the https-port info is not displayed or saved into the configuration.	None.
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 auto-negotiation 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 auto-negotiation enabled NNI port that also has non-ISIS traffic, do so during a maintenance window to minimize possible impact to other non-ISIS traffic.

Table continues…

Issue number	Description	Workaround
VOSS-4840	If you run the **`show fulltech`** command in an SSH session, do not disable SSH on the system. Doing so can block the SSH session.	None.
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-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 could 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 exhaust the NLB and Directed Broadcast shared resources. The shared resources are NLB interfaces and VLANs with

Table continues…

Issue number	Description	Workaround
		Directed Broadcast enabled. The permissible limit for the shared resources is 200.
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-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-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 | Decimal>`. This is a display issue only with no functional impact.	Use CLI to see the correct unit values.
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-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.

Table continues…

Issue number	Description	Workaround
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. The system displays this message, each time a successful SSL_Handshake occurs between the web browser and the web server. The log file cannot 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-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.

Table continues…

Issue number	Description	Workaround
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 display can cause misalignment of the output columns.	None.
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-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	Disable and re-enable Fabric Multicast (**`spbm <1-100> multicast enable`**) on the source VLAN to be able to delete the streams and come back in properly.

Table continues…

Issue number	Description	Workaround
	link. If the stream ingresses locally, it is received by the local UNI receivers.	
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 could be encountered when an exceeded amount of Application Telemetry mirrored packets are sent to the collector.	None.
VOSS-12330	When accessing 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-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 over subscription 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.
VOSS-13159	The ixgbevf Ethernet device driver within the TPVM does not correctly handle the interface MTU setting. Specifically, if you configure the interface in SR-IOV mode, packets larger than the MTU size are allowed.	To avoid this problem, configure the desired MTU size on both the relevant front-panel port and Insight port from VOSS.
VOSS-13463	Out port statistics for MLT port interfaces are not accurate.	Use the command `show io nic-counters` to display detailed port stats and error info on XA1400 Series.
VOSS-13667	An intermittent issue in SMLT environments, where ARPs or IPv6 neighbors are resolved with delay can cause a transient traffic loss for the affected IPv6 neighbors. The situation auto-corrects.	None.
VOSS-13680	Interface error statistics display is inaccurate in certain scenarios.	Use the command `show io nic-counters` to display detailed port stats and error info on XA1400 Series.

Table continues…

Issue number	Description	Workaround
VOSS-13681	QoS: show qos cosq-stats cpu-port command output is not supported.	Use the command `show io cpu-cosq-counters` to display detailed cosq-stats on XA1400 Series.
VOSS-13693	QoS: Traffic can egress out of the queue at a different ratio than the default configuration. After the guaranteed traffic rate is served to all egress port queues, any excess bandwidth is shared equally to all queues instead of distributing on weight assigned to each queue.	None.
VOSS-13702	Do not use the ACE actions of deny and mirror-to-isid together on VSP 7400 Series.	None.
VOSS-13717 VOSS-14393 VOSS-14972	Link on remote side doesn't go down after admin shut on XA1400 while using 10G DAC or a 4x10 - 40 G breakout DAC. On the XA1400 side link goes down but Link LED shows as up. Both 10G and 4x10G DAC are not fully supported because of this issue	None for DAC and breakout cables. Because of this issue, the following optical transceivers are not supported: • AA1404036-E6 • AA1404042-E6 • C9799X4-5M
VOSS-13794	You cannot use SFTP to transfer files larger than 2 GB to a VSP switch.	Use SCP.
VOSS-13904 VOSS-13932 VOSS-16503	VSP 4900 Series has 2 GB memory in a 64-bit system so the RESTCONF VLAN scaling number is smaller than on VSP 7400 Series, which has 16 GB physical memory. Using RESTCONF on VSP4900-48P or VSP4900-24S reduces the number of port-based VLANs on those platforms: • 2,000 for VSP4900-48P with RESTCONF • 1,000 for VSP4900-24S with RESTCONF	None.
VOSS-13938	You can configure LLDP-MED on an FA-enabled port, and **`show lldp`** commands show the configuration as applied but the information is not advertized and it does not appear in **`show running-config`** output nor in config.cfg if you save the configuration	None.
VOSS-13947	After you enable MSTP-Fabric Connect Multi Homing (**`spbm 1 stp-multi-homing enable`**), you cannot view the	None.

Table continues…

Issue number	Description	Workaround
	configuration, role, or statistics for the STP virtual port.	
VOSS-13948	After you enable MSTP-Fabric Connect Multi Homing (**`spbm 1 stp-multi-homing enable`**), MSTP resiliency times are 30 to 40 seconds because the internal SPB-STP port is not fast-aging remote CMAC entries after a topology change occurs.	None.
VOSS-13974	When an 8408QQ ESM has more than two channelized ports and is rebooted, the MKA MACsec sessions on the other cards in the same box could toggle. This issue is not seen if one or two ports are channelized on the same card.	None.
VOSS-14150	CLI remote console might stop wrapping text after some usage.	Reset the CLI window or open a new remote console window.
VOSS-14391	On an VSP 8404C switch using an 8424XT ESM, on a port with MACsec connectivity, if you set Auto-Negotiation advertisements to 1000-full, and then subsequently set the advertisement to 10000-full, the link will not come up.	To avoid this issue, set the Auto-Negotiation advertisements directly to 10000-full. If you have experienced the issue, shut the port down and bring it back up.
VOSS-14494	Layer 2 VSN and Layer 3 VSN UNI to NNI traffic between two Backbone Edge Bridges does not hash to different ports of a MLT network-to-network interface. MLT hashing for XA1400 devices occurs after the mac-in-mac encapsulation is done. The hash keys used are the Backbone destination and Backbone source MAC addresses (BMAC DA and BMAC SA) in the Mac-in-Mac header. Even for the Transit BCB case on XA 1400 devices for NNI to NNI traffic, the MLT hash keys used are the Backbone destination and Backbone source MAC addresses (BMAC DA and BMAC SA) in the Mac-in-Mac header.	None.
VOSS-14515	Console output errors and warnings are shown during an XA1400 Series reboot, such as: • error: no such device: ((hd0,gpt1)/EFI/BOOT)/EFI/BOOT/grub.cfg.	None. The errors or warnings are host OS or guest OS related with no functional impact and can be ignored.

Table continues…

Issue number	Description	Workaround
	error: file `/EFI/BOOT/grubenv' not found • error: no suitable video mode found. • [0.727012] ACPI: No IRQ available for PCI Interrupt Link [LNKS]. Try pci=noacpi or acpi=off • exportfs: can't open /etc/exports for reading • KCORE: WARNING can't find /boot/b/uImage-gemini.bin. No kexec kernel will be configured.	
VOSS-14590	ISIS logical-interface displays the same egress port for different tunnels when the underlay reachability is from different port interfaces.	None.
VOSS-14597	Ping (originated from local CP) fails for jumbo frames on Layer 3 VSN interface.	None.
VOSS-14616	Seeing Queue buffer usage logs when changing the logical interface source IP with 64 tunnels. When changing the source IP with 64 tunnels, seeing "GlobalRouter CPU INFO CPP: 60 percent of fbufs are in use: 0 in Tx queue,1843 in RxQueue0 0 in RxQueue1 0 in RxQueue2 0 in RxQueue3 0 in RxQueue4 0 in RxQueue5 0 in RxQueue6 0 in RxQueue7 ".	None.
VOSS-14656	Console output "ErrLog: Error Level=2 [(null)] seen during OpenVas testing. No functional impact.	None.
VOSS-14694	On a 25 Gb interface, auto-negotiation and Forward Error Correction between EXOS and VOSS platforms do not work.	None.
VOSS-14805 VOSS-15305	The following transceivers are not supported on XA1400 Series switches: • 10 Gb Bidirectional 40 km SFP+ Module (10GB-BX40-D and 10GBBX40-U) • 1000BASE-BX10 Bidirectional 10 km DDI SFP Modules (AA1419069-E6 and AA1419070-E6)	Use only supported transceivers.
VOSS-15079	The Extreme Networks 10 meter SFP+ passive copper DAC (Model Number	Use the Extreme Networks SFP+ active optical DAC (Model Number AA1403018-E6) with the VIM5-4X.

Table continues…

Issue number	Description	Workaround
	10307) does not function on ports 2/3 and 2/4 of the VIM5-4X.	
VOSS-15112	BFD sessions associated with static routes could flap one time before remaining up, when shutting down and bringing back up a BFD peer port.	None. Ignore the extra BFD session flap.
VOSS-15313	On an VSP 8404C switch using an 8424XT ESM, on a link with MACsec connectivity on both ends, and Auto-Negotiation advertisements set to 10000-full, the link will not come back up if the ESM is hot-swapped or the slot is reset.	To avoid this issue, disable MACsec prior to the hot swap or reset, and then re-enable. If you have experienced the issue, shut either one of the link ports down and bring it back up.
VOSS-15391	An SNMP walk on the **`rcIgmpSnoopTraceTable`** table will fail with an **`OID not increasing`** error. CLI and EDM are unaffected by this issue.	None.
VOSS-15463	XA1440 and XA1480 switches could experience intermittent Link Up and Link Down transitions on the 10/100/1000BASE-T Ethernet ports upon booting.	No workaround, but there is no functional impact.
VOSS-15541	You could experience temporary traffic loss when shutting down an LACP SMLT port (and therefore causing the local SMLT to go down), in a network with scaled Multicast traffic over an SPB cloud, while the datapath processes all dpm letter messages during LCAP recovery. This slow LACP recovery situation is only seen with scaled Multicast traffic over an SPB cloud.	Use static MLTs.
VOSS-15605	When you delete the VLAN IDs from the assigned I-SID of two vIST peers, the second VLAN ID deletion triggers log report **`0x0013851e`** from the first peer, indicating that a Layer 3 MAC address deletion has failed.	No workaround, but there is no functional impact—the MAC address was deleted when the VLAN:ISID association was deleted.
VOSS-15720	During key refresh events for MKA dynamic SAKs, you could experience 3-4 msec packet drops, depending on the interface line rate, incoming packet size, and incoming packet rate. Under average conditions, on a 1 Gbps port, there could be an average packet loss of 20 msec over a 24 hour period, while on a 10 Gbps port,	None. Packet loss during key refresh events is very minimal (approximately 3-4 msec). If applications cannot tolerate this amount of traffic loss also, it is advisable to use Static SAKs instead of dynamic SAKs.

Table continues…

Issue number	Description	Workaround
	there could be an average packet loss of 160 msec over a 24 hour period.	
VOSS-15812	L3VSN IPv4 BGP (and static) routes having their next-hops resolved via IS-IS routes could result in traffic loss.	Choose the following workarounds, based on your deployment and needs: • Use static routes to reach the loopbacks used as BGP peers, (static routes having better preference than IS-IS); use static routes with next-hops reachable on the UNI side (L2VSN). • Use OSPF to reach the loopbacks used as BGP peers, but take care to ensure that the OSPF route towards the BGP peer is chosen as the “best route” (as IS-IS has a better preference than OSPF). There are several ways to accomplish this—either don’t redistribute that route in IS-IS if it is not needed, or control the redistribution with a route-map, etc. • Have BGP peers reachable directly via a C-VLAN; do not use loopback interfaces as BGP peer addresses. • If none of the above workaround scenarios are suitable for your deployment, do not use internal Border Gateway Protocol (iBGP) peering.
VOSS-16221	Layer 2 ping is not working for packets larger than 1300 on an XA1400 Series.	Use Layer 2 ping with packets smaller than 1300 bytes.
VOSS-16365	Running the command **`show pluggable-optical-module detail`** on an XA1400 Series device is highly CPU intensive to read and reply with the EEPROM details. Due to a delay in ethtool response, a watchdog miss event can occur and the event is recorded in the /intflash/wd_stats/1/wd_stats.ssio.1.log file. This scenario occurs more often if 10Gb SFP+ optics with DDM capability are installed.	None. The high CPU usage and response delay for this command is expected and cannot be resolved. No console log is generated. When the scenario occurs, the Watchdog outage is approximately 5 seconds.
VOSS-16436	Using the console connection on an XA1400 Series device while running a show command with large data output can result in drops of processing control packets.	Use Telnet or SSH connectivity instead of console connection.

Table continues…

Issue number	Description	Workaround
VOSS-16951	On a VSP4900-48P, VSP4900-24S and VSP 7400 Series devices, if you run the **`show boot config sio`** CLI command before you have configured the baud rate, the output of the command is empty.	Configure the baud rate before you run the **`show boot config sio`** command. The only supported baud rate for the these devices is 115200.
VOSS-16971	On VSP4900-24S, VSP4900-24XE, andVSP4900-12MXU-12XE devices, and on the VIM5-4XE, if a copper SFP is plugged in with the cable inserted and the remote end is also plugged in, the peer box could see a link flap and take 6-8 seconds to link up.	First, plug in the SFP, and then insert the cable. The link up then happens in 3-4 seconds.
VOSS-17002	For ingress packets that are larger than the system MTU size on XA1400 Series ports 1/1 through 1/4, error counters do not increment in the **`show interfaces gigabitethernet error`** CLI command.	Use the **`show io nic-counters`** CLI command to verify if the tx_error counters are getting incremented. If they are getting incremented, the packets are getting dropped at egress. If they are not getting incremented, the packets are getting forwarded.
VOSS-17146	A small memory leak can occur in rare scenarios where static routes are used with a PIM gateway. This issue does not occur in typical scenarios that use Multicast Source Discovery Protocol (MSDP) with a PIM gateway.	None.
VOSS-17279	In a Fabric Attach network scenario with an Ethernet Routing Switch (ERS) stack connected to a VSP switch, if the ERS base unit goes down, a traffic loss between the VSP switch and the clients connected in the remaining units of the ERS stack could occur.	None.
VOSS-17429	For XA1400 Series devices connected to an FE tunnel over IPsec in a dual NAT scenario, if the IPsec responder is rebooted continuously multiple times, the tunnel cannot come back up.	Manually disable and then re-enable IPsec under the Initiator's ISIS logical interface.
VOSS-17478	On 1 G-capable VSP 4900 Series devices, the platform MACsec statistics cannot match the port Interface statistics after Key expiry.	No Workaround. This is a Statistics data issue where the expired SA Packets Counts are removed and not accounted. There is no packet loss, and no errors.
VOSS-17523	If an FE tunnel goes down between two connected XA1400 Series devices, an MTU Warning console message is logged	You can safely ignore this warning message.

Table continues…

Issue number	Description	Workaround
	if a ping request is issued while the tunnel is down.	
VOSS-17567	Do not use the inter-vrf /32 static routes defined with a next-hop IP address, that resides in a different destination next-hop-vrf context.	None.
VOSS-18023	The management port on the 5520 switch does not support Auto-MDIX (the automatic detection of transmit and received twisted pairs). It is recommended that the default auto-negotiation setting on the management port remain enabled. Because the management port does not support Auto-MDIX, when auto-negotiation is disabled, a crossover cable might be necessary in order to have the port link up and pass traffic. **Note:** If the peer device supports Auto-MDIX, then either a straight through or crossover will work. The issue occurs only if both ends of the connection do not support Auto-MDIX.	None.
VOSS-18238	When a management VLAN with DHCP is used to reach a RADIUS server, and the RADIUS server cannot be reached, the system waits for 15 minutes before attempting to reach the RADIUS server again. This is true even if the RADIUS server becomes reachable before the 15 minutes have elapsed.	None.
VOSS-18278	On the 5520 switch, when you make any change relating to port speed, the port statistics are cleared. This is applies to all front panel fiber and copper ports as well as VIM ports. The following are examples of changes relating to port speed: • Changing the auto-negotiation configuration settings on a copper port • Different negotiated speed on a copper port	None.

Table continues…

Issue number	Description	Workaround
	• Changing out an optical device for one having a different speed, for example changing from 1 Gb to 10 Gb	
VOSS-18360	This is an intermittent issue on the VSP 7400 Series with no impact to functionality, ISIS is disabled while the **`show fulltech`** command is running on a telnet session. Due to this the fulltech command will not find the expected I-SID value, as it is removed by the **`no isis`** command.	None.
VOSS-18452	On a pair of VSP 4900 Series switches, which act as Split BEBs plus PIM Gateways in a setup. Certain IPSC multicast interfaces stop working after resetting certain neighboring devices. All interfaces that are not working, reside on the LACP SMLTs.	• Run the **`no ip spb-multicast enable`** or **`ip spb-multicast enable`** commands to bounce the multicast interface, which recovers the traffic as joins are learned again. • Bounce the SMLT ports on which the VLANs that are not working reside.
VOSS-18477	On the VSP 4900 Series, an intermittent traffic loss over the FE tunnels, in SMLT contexts, occurs for a few seconds, when you read ports to the SMLT trunk.	None.
VOSS-18486	MACsec cannot be enabled on 100 Mb links of multirate ports on the 5520-12MW-36W switch. Customers who want to secure their 100 Mb links must use only ports 1/1 to 1/36. Ports 1/37 to 1/48 cannot be used for this purpose.	Use ports 1/1 to 1/36 on the 5520-12MW-36W chassis wherever 100 Mb ports need to be secured with MACsec. Alternatively, do not enable MACsec when the port speed is 100 Mb on multirate ports 1/37 to 1/48.
VOSS-18836	When you display dynamic ARP entries on VLANs, the switch displays invalid values for ipNetToMediaIfIndex. If Extreme Management Center is monitoring the switch, it can include these values when displaying AEP information to the user.	None.
VOSS-18909	Cisco 7821 IP phones might not be able to auto-negotiate to 100Mbps when connected to 1G copper ports. Instead, the connection occurs at 10Mbps.	Disable auto-negotiation on the switch and on the phone, and manually configure both sides to 100Mbps.
VOSS-19139	Immediately after you configure a new VLAN using the ZTP+ functionality available in Extreme Management Center (XMC), and you intend to use the new VLAN as management interface, you might see that all ports have been given the PVID of the new management VLAN.	This condition is temporary: Switch configuration will be finalized after discovery though ZTP+ is performed and the initial provisioning is completed. If you start the ZTP+ process though the Out of Band interface, you should complete

Table continues…

Issue number	Description	Workaround
		the onboarding using the same management interface. If you start the ZTP+ process from the management VLAN 4048, create a new VLAN during onboarding and use the new VLAN as the management interface.
VOSS-19212	After upgrading a VSP 7432CQ switch to VOSS 8.2.5 and rebooting, the presence of a faulty power supply unit will cause the system to terminate. A message in the debug log will report that the software could not read the contents of the power supply's EEPROM (*carbonatelib_ps_read_eeprom* operation).	Replace the power supply unit in the switch.
VOSS-19253	On 5520 switches, authentication is not allowed for requesters that use the switch's MAC address as destination rather than using the 802.1x reserved MAC address.	None.
VOSS-19255	For 5520 switches, the output of the **`show software`** command displays an incorrect release name for VOSS 8.2.5.	To display the correct release name, use the **`show sys-info`** or **`show sys software`** command.
VOSS-19551	The DHCP relay scale on VSP 7200, VSP 8200, and VSP 8404 is reduced to 1024 from 2048 in VOSS 8.2.	None.
VOSS-19827	LLDP IPv6 neighbors do not display in EDM. LLDP IPv6 is only supported in CLI.	To display LLDP IPv6 neighbors, use the **`show lldp neighbor summary`** command.

Restrictions and Expected Behaviors

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

For Port Mirroring considerations and restrictions, see Troubleshooting VOSS.

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 Integrated Application Hosting virtual machine using **`virtual-service tpvm console`** and use the Nano text editor	None.

Table continues…

Issue number	Description	Workaround
	inside the console access, the command **^o<cr>** does not write the file to disk.	
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 displays 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, 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.	There is no functional impact due to this configuration and it only leads to an unnecessary configuration step. No workaround required.
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	As a workaround, perform one of the following tasks: • Clear the non-EAP session on the port that the client is first

Table continues…

Issue number	Description	Workaround
	another EAPoL or Non-EAP enabled port.	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-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-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-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

Table continues…

Issue number	Description	Workaround
	replication remote peer IP and OOB Management IP.	the OOB Management IP address as the replication remote peer IP address.
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
VOSS-17871	Starting with VOSS 8.1.5, internal system updates have resulted in a more accurate accounting of memory utilization. This can result in a higher baseline memory utilization reported although actual memory usage is not impacted.	Update any network management alarms that are triggered by value with the new baseline.

Table continues…

Issue number	Description	Workaround
VOSS-18523	When you configure a port using Zero Touch Provisioning Plus (ZTP+) with Extreme Management Center, the port cannot be part of both a tagged VLAN and an untagged VLAN.	n/a
VOSS-18409	On the XA1400 Series switches, only one Central Processing Unit (CPU) core is assigned for control plane protocol processing. In a highly scaled scenario, a port toggling or negative scenario keeps the CPU core busy in updating the software datapath entries. Similarly, some show CLI commands that require a lot of data gathering keep the CPU core busy. In such a scenario, the main task which is responsible for handling protocol packets like Bidirectional Forwarding Detection, Intermediate-System-to-Intermediate-System, Virtual Link Aggregation Control Protocol, and so on is busy.	For scaled scenarios on XA1400 Series switches, the CLI commands that have large sections of output, for example, show fulltech, show io spb tables, and show tech, the output must be redirected into a file.
VOSS-18851	Do not define a static route in which the NextHop definition uses an Inter-VRF redistributed route. Such a definition would require the system to perform a double lookup. When you attempt to define a static route in this way, an error message is generated.	Define the static route in such a way that it does not require Inter-VRF redistributed routing.
VOSS-18910	On the 5520 platform in Release 8.2.5, the maximum number of forwarding Layer 2 VSNs is 3580.	n/a
VOSS-19182	The PoE power budgets for ExtremeSwitching 5520 Series switches have been reduced for the following PSU configurations: • 24W: 2x1100W PoE budget reduced from 1800W to 1781W • 48W: - 2x2000W high-line PoE budget reduced from 3600W to 3568W - 2x1100W PSU PoE budget reduced from 1800W to 1770W • 12MW-36W: - 2x2000W high-line PoE budget reduced from 3600W to 3549W	If you are using PoE on ExtremeSwitching 5520 Series switches with VOSS 8.2.5, consider the revised budget limits when deploying PoE-powered devices.

Table continues…

Issue number	Description	Workaround
	- 2x1100W PSU PoE budget reduced from 1800W to 1751W VOSS 8.2.5 enforces the previous limits. New limits will be implemented in a future release.	
VOSS-19261	For 5520 switches, low is the only valid value for the command **`boot config flags advanced-feature-bandwidth-reservation`**. (This command enables the switch to support advanced features by reserving ports as loopback ports.) In EDM, both options, low and high, are selectable. However, low is the only valid value.	When invoking the command, specify the low option.
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
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 can 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.	n/a

Table continues…

Issue number	Description	Workaround
	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.	
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. **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.	None.

Table continues…

Issue number	Description	Workaround
	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.	
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 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.	Bounce the BGP protocol globally.
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	n/a

Table continues…

Issue number	Description	Workaround
	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.	
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 workarounds: • Enable PIM on the edge. • Ensure that IST peers are either RP or DR but not both.
wi01224683 wi01224689	Additional link bounce can occur on 10 Gbps ports when toggling links or during cable re-insertion. Additional link bounce can occur with 40 Gbps optical cables and 40 Gbps break-out cables, when toggling links or during cable re-insertion.	n/a
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.

Table continues…

Issue number	Description	Workaround
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 • 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
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.
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 8.2.5 incorporates all fixes from prior releases.

Resolved Issues in VOSS 8.2.5

Issue number	Description
VOSS-17736	On XA1400 Series devices, ECMP does not work on Layer 3 VSNs when the **`system-id`** starts with "**`02.`**".
VOSS-18476	A rare issue on channelized ports on the VSP 8200 Series, LACP interfaces between the devices remain operationally down.
VOSS-18538	On the VSP 8400 Series, if you configure a static nickname that is the same as the previously assigned dynamic nickname, the nickname allocation does not change to static.
VOSS-18592	You can delete the system reserved I-SIDs (greater than 16000000) that are used by the features like Fabric Area Network and STP-Multihoming using the CLI or EDM interface. Deleting the system reserved I-SIDs could impact the system functionalities.
VOSS-18672	On the VSP 7400 Series, you cannot create a virtual port of SR-IOV and VT-d connection type using EDM.
VOSS-18741	The IPsec tunnel between the XA1480 devices with dual NAT-T, toggles with overnight traffic.

Appendix A: Related Information

MIB Changes

Deprecated MIBs

Table 34: Common

Object Name	Object OID	Deprecated in VOSS Release
rcChasForceTopologyIpFlagEnable	1.3.6.1.4.1.2272.1.4.53	8.1.60
rcChasCircuitlessIpId	1.3.6.1.4.1.2272.1.4.54	8.1.60
rcNlsMgmtAddressTable	1.3.6.1.4.1.2272.1.223.2	8.1.60
rcNlsMgmtAddressEntry	1.3.6.1.4.1.2272.1.223.2.1	8.1.60
rcNlsMgmtAddrInstanceId	1.3.6.1.4.1.2272.1.223.2.1.1	8.1.60
rcNlsMgmtIpAddress	1.3.6.1.4.1.2272.1.223.2.1.2	8.1.60
rcNlsMgmtIpMask	1.3.6.1.4.1.2272.1.223.2.1.3	8.1.60
rcNlsMgmtIpv6Address	1.3.6.1.4.1.2272.1.223.2.1.4	8.1.60
rcNlsMgmtIpv6PrefixLength	1.3.6.1.4.1.2272.1.223.2.1.5	8.1.60
rcNlsMgmtIpv6LinkLocalAddr	1.3.6.1.4.1.2272.1.223.2.1.6	8.1.60
rcNlsMgmtIntfName	1.3.6.1.4.1.2272.1.223.2.1.7	8.1.60
rcNlsScalars	1.3.6.1.4.1.2272.1.223.23	8.1.60
rcNlsMgmtDhcpClientPreferredInterface	1.3.6.1.4.1.2272.1.223.23.2	8.1.60
rcNtpGlobalInterval	1.3.6.1.4.1.2272.1.33.1.2	8.1.60
rcNtpServerTable	1.3.6.1.4.1.2272.1.33.2	8.1.60
rcNtpServerEntry	1.3.6.1.4.1.2272.1.33.2.1	8.1.60
rcNtpServerAddress	1.3.6.1.4.1.2272.1.33.2.1.1	8.1.60

Table continues…

Object Name	Object OID	Deprecated in VOSS Release
rcNtpServerEnable	1.3.6.1.4.1.2272.1.33.2.1.2	8.1.60
rcNtpServerAuthentication	1.3.6.1.4.1.2272.1.33.2.1.3	8.1.60
rcNtpServerKeyId	1.3.6.1.4.1.2272.1.33.2.1.4	8.1.60
rcNtpServerAccessAttempts	1.3.6.1.4.1.2272.1.33.2.1.5	8.1.60
rcNtpServerAccessSuccess	1.3.6.1.4.1.2272.1.33.2.1.6	8.1.60
rcNtpServerAccessFailure	1.3.6.1.4.1.2272.1.33.2.1.7	8.1.60
rcNtpServerRowStatus	1.3.6.1.4.1.2272.1.33.2.1.8	8.1.60
rcNtpServerVersion	1.3.6.1.4.1.2272.1.33.2.1.10	8.1.60
rcNtpServerRootDelay	1.3.6.1.4.1.2272.1.33.2.1.11	8.1.60
rcNtpServerReachable	1.3.6.1.4.1.2272.1.33.2.1.13	8.1.60
rcNtpServerSynchronized	1.3.6.1.4.1.2272.1.33.2.1.14	8.1.60
rcNtpServerSourceIpAddr	1.3.6.1.4.1.2272.1.33.2.1.15	8.1.60
rcSysAccessPolicyTrustedHostUserName	1.3.6.1.4.1.2272.1.1.61.1.10	8.1.60
rcNtpGlobalVersion	1.3.6.1.4.1.2272.1.33.1.7	8.1.60
rc2kBootConfigEnableRloginServer	1.3.6.1.4.1.2272.1.100.5.1.17	8.1.60
rc2kBootConfigInsightPortConnectType	1.3.6.1.4.1.2272.1.100.5.1.61	8.1.60
rcKhiCppProtocolDropsRshCnt	1.3.6.1.4.1.2272.1.85.12.5.16	8.1.60
rcKhiCppProtocolDropsRloginCnt	1.3.6.1.4.1.2272.1.85.12.5.58	8.1.60
rcCliMaxTelnetSessions	1.3.6.1.4.1.2272.1.19.11	8.2
rcSyslogGlobalHeader	1.3.6.1.4.1.2272.1.22.1.4	8.2
rcNtpGlobalVersion	1.3.6.1.4.1.2272.1.33.1.7	8.2
rcIsisGlobalMgmtIpAddr	1.3.6.1.4.1.2272.1.63.1.21	8.2
rcKhiCppProtocolDropsRshCnt	1.3.6.1.4.1.2272.1.85.12.5.16	8.2
rcKhiCppProtocolDropsRloginCnt	1.3.6.1.4.1.2272.1.85.12.5.58	8.2
rc2kBootConfigEnableRloginServer	1.3.6.1.4.1.2272.1.100.5.1.17	8.2
rcCloudIqNotificationEnable	1.3.6.1.4.1.2272.1.230.1.1.10	8.2

Modified MIBs

Table 35: Common

Object Name	Object OID	Modified in VOSS Release	Modification
rcPortType	1.3.6.1.4.1.2272.1.4.10.1.1.2	8.1	ADD_ENUM: 195-212
rcVossSystemVimAdminSpeed	1.3.6.1.4.1.2272.1.101.1.1.1.3	8.1	ADD_ENUM: unsupported(3)
rcVossSystemCardLedId	1.3.6.1.4.1.2272.1.101.1.1.5.1.2	8.1	CHANGE_RANGE: Changed the range from 1..5 to 1..9
rcSysDnsServerListType	1.3.6.1.4.1.2272.1.1.64.1.1	8.1.60	Added the following fields to support dynamic servers: • primaryDynamic • secondaryDynamic • tertiaryDynamic
rcNIsMgmtIpRouteType	1.3.6.1.4.1.2272.1.223.8.1.7	8.1.60	Added the following value: • dhcp(4)
SnpxChassisType		8.2.5	ADD ENUM: m552048TVOSS, m552048WVOSS, m552012MW36WVOSS, m552024TVOSS, m552024WVOSS, m552024XVOSS, m552048SEVOSS
rcChasType	1.3.6.1.4.1.2272.1.4.1	8.2.5	ADD ENUM: a552024TVOSS, a552024WVOSS, a552048TVOSS, a552048WVOSS, a552012MW36WVOSS, a552048SEVOSS, a552024XVOSS
rc2kCardFrontType	1.3.6.1.4.1.2272.1.100.6.1.2	8.2.5	ADD ENUM: voss5520x24T, voss5520x24W, voss5520x48T, voss5520x48W, voss5520x12MW36W, voss5520x48SE, voss5520x24X, voss5520x4X
rcLicenseLicenseType	1.3.6.1.4.1.2272.1.56.4	8.2.5	ADD_ENUM: macsec(15)

Table 36: 5520 Series

Object Name	Object OID	Modified in VOSS Release	Modification
bnIfExtnPoweredDeviceDetectType	1.3.6.1.4.1.45.1.6.15.1.1.1.6	8.2.5	ADD_ENUM: compliantWith802dot3btType3(5), compliantWith802dot3btType4(6)
bspePethPsePortExtPowerLimit	1.3.6.1.4.1.45.5.8.1.1.1.5	8.2.5	CHANGE_RANGE: from 64 to 98
bspePethPsePortExtMeasuredCurrent	1.3.6.1.4.1.45.5.8.1.1.1.6	8.2.5	CHANGE_RANGE: from 1200 to 1920
bspePethPsePortExtMeasuredPower	1.3.6.1.4.1.45.5.8.1.1.1.7	8.2.5	CHANGE_RANGE: from 64000 to 98000
rc2kChassisPortLed3Status	1.3.6.1.4.1.2272.1.100.1.14	8.2.5	ADD_NEW_VALUES: Add values for speed and activity for VSP5520
rcMACSecConnectivityAssociationTxKeyParity	1.3.6.1.4.1.2272.1.88.1.1.6	8.2.5	REMOVED none(1) value
rcSysActionL	1 1.3.6.1.4.1.2272.1.1.86	8.2.5	ADD_ENUM: revokeLicensePremier(12), revokeLicenseMacsec(12)

Table 37: XA1400 Series

Object Name	Object OID	Modified in VOSS Release	Modification
rcIsisGlobalIpTunnelMtu	. 1.3.6.1.4.1.2272.1.63.1.20.0	8.1	CHANGE_RANGE: Changed the range from 750..1950 to 750..9000
rcIsisLogicalInterfaceShapingRate	1.3.6.1.4.1.2272.1.63.26.1.16	8.1	CHANGE_RANGE: Changed the range from 0..5000 to 0..1000. Changed the type from Integer32 to INTEGER.
rcCfmTransmitL2IpPingIpAddrType	1.3.6.1.4.1.2272.1.69.37.1.1	8.1.1	Supports only Ipv4 address type.
rcCfmTransmitL2IpPingIpAddr	1.3.6.1.4.1.2272.1.69.37.1.2	8.1.1	Supports only ipv4 address.
rcIpsecPolicyDstAddressType	1.3.6.1.4.1.2272.1.213.1.1.2	8.1.1	Supports only Ipv4 address type.

Table continues…

Object Name	Object OID	Modified in VOSS Release	Modification
rcIpsecPolicyDstAddress	1.3.6.1.4.1.2272.1.213.1.1.3	8.1.1	Supports only ipv4 address.
rcIpsecPolicySrcAddressType	1.3.6.1.4.1.2272.1.213.1.1.4	8.1.1	Supports only Ipv4 address type.
rcIpsecPolicySrcAddress	1.3.6.1.4.1.2272.1.213.1.1.5	8.1.1	Supports only ipv4 address.
rcIpsecPolicyL4Protocol	1.3.6.1.4.1.2272.1.213.1.1.9	8.1.1	Supports only tcp(6), udp(17) and icmp(1) values.
rcIpRedistributeInterVrfProtocol	1.3.6.1.4.1.2272.1.8.100.22.1.2	8.1.1	Supports only ospf(1), bgp(2), isis(3), vrf-ext(4) and rip(6) values.
rcIpRedistributeInterVrfRouteSource	1.3.6.1.4.1.2272.1.8.100.22.1.4	8.1.1	Supports only direct(1), static(2), rip(3), ospf(4), bgp(5) and isis(13) values.
rcCfmTransmitL2IpTraceIpAddrType	1.3.6.1.4.1.2272.1.69.39.1.1	8.1.1	Supports only ipv4 address type.
rcCfmTransmitL2IpTraceIpAddr	1.3.6.1.4.1.2272.1.69.39.1.2	8.1.1	Supports only ipv4 address.
rcPortIngressRateLimit	1.3.6.1.4.1.2272.1.4.10.1.1.85	8.1.50	Supports 10000000 maximum value.
rmon	1.3.6.1.2.1.16	8.2	REACTIVATE: Supports RMON2 on MicroVSP.
rc2kChassisPortLed3Status	1.3.6.1.4.1.2272.1.100.1.14	8.2	ADD_NEW_VALUES: Add values for speed and activity for XA1400.

New MIBs

Table 38: Common

Object Name	Object OID	New in VOSS Release
rcNlsMgmtAddressTable	1.3.6.1.4.1.2272.1.223.2	8.1.1
rcNlsMgmtIpArpTable	1.3.6.1.4.1.2272.1.223.3	8.1.1
rcNlsMgmtIpStaticRouteTable	1.3.6.1.4.1.2272.1.223.5	8.1.1
rcNlsMgmtStatsTable	1.3.6.1.4.1.2272.1.223.7	8.1.1
rcNlsMgmtIpRouteTable	1.3.6.1.4.1.2272.1.223.8	8.1.1
rcCloudIq	1.3.6.1.4.1.2272.1.230	8.1.1

Table continues…

Object Name	Object OID	New in VOSS Release
rcCloudIqObjects	1.3.6.1.4.1.2272.1.230.1	8.1.1
rcCloudIqScalars	1.3.6.1.4.1.2272.1.230.1.1	8.1.1
rcCloudIqAgentEnable	1.3.6.1.4.1.2272.1.230.1.1.1	8.1.1
rcCloudIqAgentVersion	1.3.6.1.4.1.2272.1.230.1.1.2	8.1.1
rcCloudIqServerAddressType	1.3.6.1.4.1.2272.1.230.1.1.3	8.1.1
rcCloudIqServerAddress	1.3.6.1.4.1.2272.1.230.1.1.4	8.1.1
rcCloudIqProxyAddressType	1.3.6.1.4.1.2272.1.230.1.1.5	8.1.1
rcCloudIqProxyAddress	1.3.6.1.4.1.2272.1.230.1.1.6	8.1.1
rcCloudIqProxyTcpPort	1.3.6.1.4.1.2272.1.230.1.1.7	8.1.1
rcCloudIqProxyUserName	1.3.6.1.4.1.2272.1.230.1.1.8	8.1.1
rcCloudIqProxyPassword	1.3.6.1.4.1.2272.1.230.1.1.9	8.1.1
rcCloudIqNotificationEnable	1.3.6.1.4.1.2272.1.230.1.1.10	8.1.1
rcCloudIqOperStatus	1.3.6.1.4.1.2272.1.230.1.1.11	8.1.1
rcCloudIqAssociationUrl	1.3.6.1.4.1.2272.1.230.1.1.12	8.1.1
rcCloudIqPollUrl	1.3.6.1.4.1.2272.1.230.1.1.13	8.1.1
rcCloudIqMonitorFreq	1.3.6.1.4.1.2272.1.230.1.1.14	8.1.1
rcCloudIqPollFreq	1.3.6.1.4.1.2272.1.230.1.1.15	8.1.1
rcCloudIqLastOnboardTime	1.3.6.1.4.1.2272.1.230.1.1.16	8.1.1
rcCloudIqLastPollStatus	1.3.6.1.4.1.2272.1.230.1.1.17	8.1.1
rcCloudIqLastPollTime	1.3.6.1.4.1.2272.1.230.1.1.18	8.1.1
rcCloudIqLastMonitorStatus	1.3.6.1.4.1.2272.1.230.1.1.19	8.1.1
rcCloudIqLastMonitorTime	1.3.6.1.4.1.2272.1.230.1.1.20	8.1.1
rcCloudIqLastHealthStatus	1.3.6.1.4.1.2272.1.230.1.1.21	8.1.1
rcCloudIqLastHealthTime	1.3.6.1.4.1.2272.1.230.1.1.22	8.1.1
rcnCloudIqUpTrap	1.3.6.1.4.1.2272.1.21.0.357	8.1.1
rcnCloudIqDownTrap	1.3.6.1.4.1.2272.1.21.0.358	8.1.1
bspePethPsePortExtFastPoeEnable	1.3.6.1.4.1.45.5.8.1.1.1.13	8.1.5
bspePethPsePortExtPerpetualPoeEnable	1.3.6.1.4.1.45.5.8.1.1.1.14	8.1.5
bspePethMainPseFastPoeEnable	1.3.6.1.4.1.45.5.8.1.2.1.4	8.1.5
bspePethMainPsePerpetualPoeEnable	1.3.6.1.4.1.45.5.8.1.2.1.5	8.1.5
rcNlsMgmtInterfaceRmonAdminEnable	1.3.6.1.4.1.2272.1.223.1.1.12	8.1.60
rcNlsMgmtInterfaceRmonOperEnable	1.3.6.1.4.1.2272.1.223.1.1.13	8.1.60
rcNlsMgmtInterfaceRmonIpAddress	1.3.6.1.4.1.2272.1.223.1.1.14	8.1.60
rcNlsMgmtKhiStatsTable	1.3.6.1.4.1.2272.1.223.21	8.1.60
rcNlsMgmtKhiStatsEntry	1.3.6.1.4.1.2272.1.223.21.1	8.1.60

Table continues…

Object Name	Object OID	New in VOSS Release
rcNlsMgmtKhiStatsInstanceId	1.3.6.1.4.1.2272.1.223.21.1.1	8.1.60
rcNlsMgmtKhiStatsPacketType	1.3.6.1.4.1.2272.1.223.21.1.2	8.1.60
rcNlsMgmtKhiStatsPacketName	1.3.6.1.4.1.2272.1.223.21.1.3	8.1.60
rcNlsMgmtKhiStatsRxPackets	1.3.6.1.4.1.2272.1.223.21.1.4	8.1.60
rcNlsMgmtKhiStatsTxPackets	1.3.6.1.4.1.2272.1.223.21.1.5	8.1.60
rcNlsMgmtKhiStatsRxDropped	1.3.6.1.4.1.2272.1.223.21.1.6	8.1.60
rcNlsMgmtKhiStatsClear	1.3.6.1.4.1.2272.1.223.22	8.1.60
rcNlsMgmtIpStats	1.3.6.1.4.1.2272.1.223.14	8.1.60
rcNlsMgmtIpv6Stats	1.3.6.1.4.1.2272.1.223.15	8.1.60
rcNlsMgmtIpStatsClear	1.3.6.1.4.1.2272.1.223.14.18	8.1.60
rcNlsMgmtIp6StatsClear	1.3.6.1.4.1.2272.1.223.15.33	8.1.60
rcNlsMgmtIpStatsInReceives	1.3.6.1.4.1.2272.1.223.14.1	8.1.60
rcNlsMgmtIpStatsInHdrErrors	1.3.6.1.4.1.2272.1.223.14.2	8.1.60
rcNlsMgmtIpStatsInAddrErrors	1.3.6.1.4.1.2272.1.223.14.3	8.1.60
rcNlsMgmtIpStatsInUnknownProtos	1.3.6.1.4.1.2272.1.223.14.4	8.1.60
rcNlsMgmtIpStatsInDiscards	1.3.6.1.4.1.2272.1.223.14.5	8.1.60
rcNlsMgmtIpStatsInDelivers	1.3.6.1.4.1.2272.1.223.14.6	8.1.60
rcNlsMgmtIpStatsOutRequests	1.3.6.1.4.1.2272.1.223.14.7	8.1.60
rcNlsMgmtIpStatsOutDiscards	1.3.6.1.4.1.2272.1.223.14.8	8.1.60
rcNlsMgmtIpStatsOutNoRoutes	1.3.6.1.4.1.2272.1.223.14.9	8.1.60
rcNlsMgmtIpStatsForwDatagrams	1.3.6.1.4.1.2272.1.223.14.10	8.1.60
rcNlsMgmtIpStatsReasmTimeout	1.3.6.1.4.1.2272.1.223.14.11	8.1.60
rcNlsMgmtIpStatsReasmReqds	1.3.6.1.4.1.2272.1.223.14.12	8.1.60
rcNlsMgmtIpStatsReasmOKs	1.3.6.1.4.1.2272.1.223.14.13	8.1.60
rcNlsMgmtIpStatsReasmFails	1.3.6.1.4.1.2272.1.223.14.14	8.1.60
rcNlsMgmtIpStatsFragOKs	1.3.6.1.4.1.2272.1.223.14.15	8.1.60
rcNlsMgmtIpStatsFragFails	1.3.6.1.4.1.2272.1.223.14.16	8.1.60
rcNlsMgmtIpStatsFragCreates	1.3.6.1.4.1.2272.1.223.14.17	8.1.60
rcNlsMgmtIp6StatsInReceives	1.3.6.1.4.1.2272.1.223.15.1	8.1.60
rcNlsMgmtIp6StatsInHdrErrors	1.3.6.1.4.1.2272.1.223.15.2	8.1.60
rcNlsMgmtIp6StatsInAddrErrors	1.3.6.1.4.1.2272.1.223.15.3	8.1.60
rcNlsMgmtIp6StatsInUnknownProtos	1.3.6.1.4.1.2272.1.223.15.4	8.1.60
rcNlsMgmtIp6StatsInDiscards	1.3.6.1.4.1.2272.1.223.15.5	8.1.60
rcNlsMgmtIp6StatsInDelivers	1.3.6.1.4.1.2272.1.223.15.6	8.1.60
rcNlsMgmtIp6StatsInTooBigErrors	1.3.6.1.4.1.2272.1.223.15.7	8.1.60

Table continues…

Object Name	Object OID	New in VOSS Release
rcNlsMgmtIp6StatsInNoRoutes	1.3.6.1.4.1.2272.1.223.15.8	8.1.60
rcNlsMgmtIp6StatsInTruncatedPkts	1.3.6.1.4.1.2272.1.223.15.9	8.1.60
rcNlsMgmtIp6StatsInMcastPkts	1.3.6.1.4.1.2272.1.223.15.10	8.1.60
rcNlsMgmtIp6StatsInOctets	1.3.6.1.4.1.2272.1.223.15.11	8.1.60
rcNlsMgmtIp6StatsInMcastOctets	1.3.6.1.4.1.2272.1.223.15.12	8.1.60
rcNlsMgmtIp6StatsInBcastOctets	1.3.6.1.4.1.2272.1.223.15.13	8.1.60
rcNlsMgmtIp6StatsInNoECTPkts	1.3.6.1.4.1.2272.1.223.15.14	8.1.60
rcNlsMgmtIp6StatsInECT1Pkts	1.3.6.1.4.1.2272.1.223.15.15	8.1.60
rcNlsMgmtIp6StatsInECT0Pkts	1.3.6.1.4.1.2272.1.223.15.16	8.1.60
rcNlsMgmtIp6StatsInCEPkts	1.3.6.1.4.1.2272.1.223.15.17	8.1.60
rcNlsMgmtIp6StatsOutRequests	1.3.6.1.4.1.2272.1.223.15.18	8.1.60
rcNlsMgmtIp6StatsOutDiscards	1.3.6.1.4.1.2272.1.223.15.19	8.1.60
rcNlsMgmtIp6StatsOutNoRoutes	1.3.6.1.4.1.2272.1.223.15.20	8.1.60
rcNlsMgmtIp6StatsOutForwDatagrams	1.3.6.1.4.1.2272.1.223.15.21	8.1.60
rcNlsMgmtIp6StatsOutMcastPkts	1.3.6.1.4.1.2272.1.223.15.22	8.1.60
rcNlsMgmtIp6StatsOutOctets	1.3.6.1.4.1.2272.1.223.15.23	8.1.60
rcNlsMgmtIp6StatsOutMcastOctets	1.3.6.1.4.1.2272.1.223.15.24	8.1.60
rcNlsMgmtIp6StatsOutBcastOctets	1.3.6.1.4.1.2272.1.223.15.25	8.1.60
rcNlsMgmtIp6StatsReasmTimeout	1.3.6.1.4.1.2272.1.223.15.26	8.1.60
rcNlsMgmtIp6StatsReasmReqds	1.3.6.1.4.1.2272.1.223.15.27	8.1.60
rcNlsMgmtIp6StatsReasmOKs	1.3.6.1.4.1.2272.1.223.15.28	8.1.60
rcNlsMgmtIp6StatsReasmFails	1.3.6.1.4.1.2272.1.223.15.29	8.1.60
rcNlsMgmtIp6StatsFragOKs	1.3.6.1.4.1.2272.1.223.15.30	8.1.60
rcNlsMgmtIp6StatsFragFails	1.3.6.1.4.1.2272.1.223.15.31	8.1.60
rcNlsMgmtIp6StatsFragCreates	1.3.6.1.4.1.2272.1.223.15.32	8.1.60
rcNlsMgmtIcmpStats	1.3.6.1.4.1.2272.1.223.16	8.1.60
rcNlsMgmtIcmp6Stats	1.3.6.1.4.1.2272.1.223.17	8.1.60
rcNlsMgmtIcmpStatsClear	1.3.6.1.4.1.2272.1.223.16.30	8.1.60
rcNlsMgmtIcmp6StatsClear	1.3.6.1.4.1.2272.1.223.17.41	8.1.60
rcNlsMgmtIcmpStatsInMsgs	1.3.6.1.4.1.2272.1.223.16.1	8.1.60
rcNlsMgmtIcmpStatsInErrors	1.3.6.1.4.1.2272.1.223.16.2	8.1.60
rcNlsMgmtIcmpStatsInCsumErrors	1.3.6.1.4.1.2272.1.223.16.3	8.1.60
rcNlsMgmtIcmpStatsInDestUnreachs	1.3.6.1.4.1.2272.1.223.16.4	8.1.60
rcNlsMgmtIcmpStatsInTimeExcds	1.3.6.1.4.1.2272.1.223.16.5	8.1.60
rcNlsMgmtIcmpStatsInParmProbs	1.3.6.1.4.1.2272.1.223.16.6	8.1.60

Table continues…

Object Name	Object OID	New in VOSS Release
rcNlsMgmtIcmpStatsInSrcQuenchs	1.3.6.1.4.1.2272.1.223.16.7	8.1.60
rcNlsMgmtIcmpStatsInRedirects	1.3.6.1.4.1.2272.1.223.16.8	8.1.60
rcNlsMgmtIcmpStatsInEchos	1.3.6.1.4.1.2272.1.223.16.9	8.1.60
rcNlsMgmtIcmpStatsInEchoReps	1.3.6.1.4.1.2272.1.223.16.10	8.1.60
rcNlsMgmtIcmpStatsInTimestamps	1.3.6.1.4.1.2272.1.223.16.11	8.1.60
rcNlsMgmtIcmpStatsInTimestampReps	1.3.6.1.4.1.2272.1.223.16.12	8.1.60
rcNlsMgmtIcmpStatsInAddrMasks	1.3.6.1.4.1.2272.1.223.16.13	8.1.60
rcNlsMgmtIcmpStatsInAddrMaskReps	1.3.6.1.4.1.2272.1.223.16.14	8.1.60
rcNlsMgmtIcmpStatsOutMsgs	1.3.6.1.4.1.2272.1.223.16.15	8.1.60
rcNlsMgmtIcmpStatsOutErrors	1.3.6.1.4.1.2272.1.223.16.16	8.1.60
rcNlsMgmtIcmpStatsOutDestUnreachs	1.3.6.1.4.1.2272.1.223.16.17	8.1.60
rcNlsMgmtIcmpStatsOutTimeExcds	1.3.6.1.4.1.2272.1.223.16.18	8.1.60
rcNlsMgmtIcmpStatsOutParmProbs	1.3.6.1.4.1.2272.1.223.16.19	8.1.60
rcNlsMgmtIcmpStatsOutSrcQuenchs	1.3.6.1.4.1.2272.1.223.16.20	8.1.60
rcNlsMgmtIcmpStatsOutRedirects	1.3.6.1.4.1.2272.1.223.16.21	8.1.60
rcNlsMgmtIcmpStatsOutEchos	1.3.6.1.4.1.2272.1.223.16.22	8.1.60
rcNlsMgmtIcmpStatsOutEchoReps	1.3.6.1.4.1.2272.1.223.16.23	8.1.60
rcNlsMgmtIcmpStatsOutTimestamps	1.3.6.1.4.1.2272.1.223.16.24	8.1.60
rcNlsMgmtIcmpStatsOutTimestampReps	1.3.6.1.4.1.2272.1.223.16.25	8.1.60
rcNlsMgmtIcmpStatsOutAddrMasks	1.3.6.1.4.1.2272.1.223.16.26	8.1.60
rcNlsMgmtIcmpStatsOutAddrMaskReps	1.3.6.1.4.1.2272.1.223.16.27	8.1.60
rcNlsMgmtIcmpStatsMsgInType0	1.3.6.1.4.1.2272.1.223.16.28	8.1.60
rcNlsMgmtIcmpStatsMsgOutType8	1.3.6.1.4.1.2272.1.223.16.29	8.1.60
rcNlsMgmtIcmp6StatsInMsgs	1.3.6.1.4.1.2272.1.223.17.1	8.1.60
rcNlsMgmtIcmp6StatsInErrors	1.3.6.1.4.1.2272.1.223.17.2	8.1.60
rcNlsMgmtIcmp6StatsInCsumErrors	1.3.6.1.4.1.2272.1.223.17.3	8.1.60
rcNlsMgmtIcmp6StatsInDestUnreachs	1.3.6.1.4.1.2272.1.223.17.4	8.1.60
rcNlsMgmtIcmp6StatsInTimeExcds	1.3.6.1.4.1.2272.1.223.17.5	8.1.60
rcNlsMgmtIcmp6StatsInParmProbs	1.3.6.1.4.1.2272.1.223.17.6	8.1.60
rcNlsMgmtIcmp6StatsInPktTooBigs	1.3.6.1.4.1.2272.1.223.17.7	8.1.60
rcNlsMgmtIcmp6StatsInRedirects	1.3.6.1.4.1.2272.1.223.17.8	8.1.60
rcNlsMgmtIcmp6StatsInEchos	1.3.6.1.4.1.2272.1.223.17.9	8.1.60
rcNlsMgmtIcmp6StatsInEchoReplies	1.3.6.1.4.1.2272.1.223.17.10	8.1.60
rcNlsMgmtIcmp6StatsInGroupMembQueries	1.3.6.1.4.1.2272.1.223.17.11	8.1.60
rcNlsMgmtIcmp6StatsInGroupMembResponses	1.3.6.1.4.1.2272.1.223.17.12	8.1.60

Table continues…

Object Name	Object OID	New in VOSS Release
rcNlsMgmtIcmp6StatsInGroupMembReductions	1.3.6.1.4.1.2272.1.223.17.13	8.1.60
rcNlsMgmtIcmp6StatsInRouterSolicits	1.3.6.1.4.1.2272.1.223.17.14	8.1.60
rcNlsMgmtIcmp6StatsInRouterAdvertisements	1.3.6.1.4.1.2272.1.223.17.15	8.1.60
rcNlsMgmtIcmp6StatsInNeighborSolicits	1.3.6.1.4.1.2272.1.223.17.16	8.1.60
rcNlsMgmtIcmp6StatsInNeighborAdvertisements	1.3.6.1.4.1.2272.1.223.17.17	8.1.60
rcNlsMgmtIcmp6StatsInMLDv2Reports	1.3.6.1.4.1.2272.1.223.17.18	8.1.60
rcNlsMgmtIcmp6StatsInType134	1.3.6.1.4.1.2272.1.223.17.19	8.1.60
rcNlsMgmtIcmp6StatsInType136	1.3.6.1.4.1.2272.1.223.17.20	8.1.60
rcNlsMgmtIcmp6StatsOutMsgs	1.3.6.1.4.1.2272.1.223.17.21	8.1.60
rcNlsMgmtIcmp6StatsOutErrors	1.3.6.1.4.1.2272.1.223.17.22	8.1.60
rcNlsMgmtIcmp6StatsOutDestUnreachs	1.3.6.1.4.1.2272.1.223.17.23	8.1.60
rcNlsMgmtIcmp6StatsOutTimeExcds	1.3.6.1.4.1.2272.1.223.17.24	8.1.60
rcNlsMgmtIcmp6StatsOutParmProbs	1.3.6.1.4.1.2272.1.223.17.25	8.1.60
rcNlsMgmtIcmp6StatsOutPktTooBigs	1.3.6.1.4.1.2272.1.223.17.26	8.1.60
rcNlsMgmtIcmp6StatsOutRedirects	1.3.6.1.4.1.2272.1.223.17.27	8.1.60
rcNlsMgmtIcmp6StatsOutEchos	1.3.6.1.4.1.2272.1.223.17.28	8.1.60
rcNlsMgmtIcmp6StatsOutEchoReps	1.3.6.1.4.1.2272.1.223.17.29	8.1.60
rcNlsMgmtIcmp6StatsOutGroupMembQueries	1.3.6.1.4.1.2272.1.223.17.30	8.1.60
rcNlsMgmtIcmp6StatsOutGroupMembResponses	1.3.6.1.4.1.2272.1.223.17.31	8.1.60
rcNlsMgmtIcmp6StatsOutGroupMembReductions	1.3.6.1.4.1.2272.1.223.17.32	8.1.60
rcNlsMgmtIcmp6StatsOutRouterSolicits	1.3.6.1.4.1.2272.1.223.17.33	8.1.60
rcNlsMgmtIcmp6StatsOutRouterAdvertisements	1.3.6.1.4.1.2272.1.223.17.34	8.1.60
rcNlsMgmtIcmp6StatsOutNeighborSolicits	1.3.6.1.4.1.2272.1.223.17.35	8.1.60
rcNlsMgmtIcmp6StatsOutNeighborAdvertisements	1.3.6.1.4.1.2272.1.223.17.36	8.1.60
rcNlsMgmtIcmp6StatsOutMLDv2Reports	1.3.6.1.4.1.2272.1.223.17.37	8.1.60
rcNlsMgmtIcmp6StatsOutType133	1.3.6.1.4.1.2272.1.223.17.38	8.1.60
rcNlsMgmtIcmp6StatsOutType135	1.3.6.1.4.1.2272.1.223.17.39	8.1.60
rcNlsMgmtIcmp6StatsOutType143	1.3.6.1.4.1.2272.1.223.17.40	8.1.60
rcNlsMgmtTcpStatsTable	1.3.6.1.4.1.2272.1.223.19	8.1.60
rcNlsMgmtTcpStatsClear	1.3.6.1.4.1.2272.1.223.19.1.12	8.1.60
rcNlsMgmtTcpStatsEntry	1.3.6.1.4.1.2272.1.223.19.1	8.1.60
rcNlsMgmtTcpStatsIPVersion	1.3.6.1.4.1.2272.1.223.19.1.1	8.1.60
rcNlsMgmtTcpStatsActiveOpens	1.3.6.1.4.1.2272.1.223.19.1.2	8.1.60
rcNlsMgmtTcpStatsPassiveOpens	1.3.6.1.4.1.2272.1.223.19.1.3	8.1.60

Table continues…

Object Name	Object OID	New in VOSS Release
rcNlsMgmtTcpStatsAttemptFails	1.3.6.1.4.1.2272.1.223.19.1.4	8.1.60
rcNlsMgmtTcpStatsEstabResets	1.3.6.1.4.1.2272.1.223.19.1.5	8.1.60
rcNlsMgmtTcpStatsInSegs	1.3.6.1.4.1.2272.1.223.19.1.6	8.1.60
rcNlsMgmtTcpStatsOutSegs	1.3.6.1.4.1.2272.1.223.19.1.7	8.1.60
rcNlsMgmtTcpStatsRetransSegs	1.3.6.1.4.1.2272.1.223.19.1.8	8.1.60
rcNlsMgmtTcpStatsInErrs	1.3.6.1.4.1.2272.1.223.19.1.9	8.1.60
rcNlsMgmtTcpStatsOutRsts	1.3.6.1.4.1.2272.1.223.19.1.10	8.1.60
rcNlsMgmtTcpStatsInCsumErrors	1.3.6.1.4.1.2272.1.223.19.1.11	8.1.60
rcNlsMgmtUdpStatsTable	1.3.6.1.4.1.2272.1.223.18	8.1.60
rcNlsMgmtUdpStatsClear	1.3.6.1.4.1.2272.1.223.18.1.10	8.1.60
rcNlsMgmtUdpStatsEntry	1.3.6.1.4.1.2272.1.223.18.1.1	8.1.60
rcNlsMgmtUdpStatsIPVersion	1.3.6.1.4.1.2272.1.223.18.1.2	8.1.60
rcNlsMgmtUdpStatsInDatagrams	1.3.6.1.4.1.2272.1.223.18.1.3	8.1.60
rcNlsMgmtUdpStatsNoPorts	1.3.6.1.4.1.2272.1.223.18.1.4	8.1.60
rcNlsMgmtUdpStatsInErrors	1.3.6.1.4.1.2272.1.223.18.1.5	8.1.60
rcNlsMgmtUdpStatsOutDatagrams	1.3.6.1.4.1.2272.1.223.18.1.6	8.1.60
rcNlsMgmtUdpStatsIgnoredMulti	1.3.6.1.4.1.2272.1.223.18.1.7	8.1.60
rcNlsMgmtUdpStatsRcvbufErrors	1.3.6.1.4.1.2272.1.223.18.1.8	8.1.60
rcNlsMgmtUdpStatsSndbufErrors	1.3.6.1.4.1.2272.1.223.18.1.9	8.1.60
rcNlsMgmtUdpStatsInCsumErrors	1.3.6.1.4.1.2272.1.223.18.1.10	8.1.60
rcNlsMgmtSocketStatisticsTable	1.3.6.1.4.1.2272.1.223.20	8.1.60
rcNlsMgmtSocketStatisticsEntry	1.3.6.1.4.1.2272.1.223.20.1	8.1.60
rcNlsMgmtSocketStatisticsIPVersion	1.3.6.1.4.1.2272.1.223.20.1.1	8.1.60
rcNlsMgmtSocketStatisticsType	1.3.6.1.4.1.2272.1.223.20.1.2	8.1.60
rcNlsMgmtSocketStatisticsIndex	1.3.6.1.4.1.2272.1.223.20.1.3	8.1.60
rcNlsMgmtSocketStatisticsState	1.3.6.1.4.1.2272.1.223.20.1.4	8.1.60
rcNlsMgmtSocketStatisticsRecvQ	1.3.6.1.4.1.2272.1.223.20.1.5	8.1.60
rcNlsMgmtSocketStatisticsSendQ	1.3.6.1.4.1.2272.1.223.20.1.6	8.1.60
rcNlsMgmtSocketStatisticsLocalAddressAndPort	1.3.6.1.4.1.2272.1.223.20.1.7	8.1.60
rcNlsMgmtSocketStatisticsPeerAddressAndPort	1.3.6.1.4.1.2272.1.223.20.1.8	8.1.60
rcRadiusGlobalSecureEnable	1.3.6.1.4.1.2272.1.29.1.26	8.1.60
rcRadiusServHostSecureEnable	1.3.6.1.4.1.2272.1.29.5.1.31	8.1.60

Table continues…

Object Name	Object OID	New in VOSS Release
rcRadiusServHostSecureMode	1.3.6.1.4.1.2272.1.29.5.1.32	8.1.60
rcRadiusServHostSecureProfile	1.3.6.1.4.1.2272.1.29.5.1.33	8.1.60
rcRadiusServHostSecureLogLevel	1.3.6.1.4.1.2272.1.29.5.1.34	8.1.60
rcRadiusSecureProfileTable	1.3.6.1.4.1.2272.1.29.9	8.1.60
rcRadiusSecureProfileEntry	1.3.6.1.4.1.2272.1.29.9.1	8.1.60
rcRadiusSecureProfileName	1.3.6.1.4.1.2272.1.29.9.1.1	8.1.60
rcRadiusSecureProfileRootCert	1.3.6.1.4.1.2272.1.29.9.1.2	8.1.60
rcRadiusSecureProfileCert	1.3.6.1.4.1.2272.1.29.9.1.3	8.1.60
rcRadiusSecureProfileKey	1.3.6.1.4.1.2272.1.29.9.1.4	8.1.60
rcRadiusSecureProfilePassword	1.3.6.1.4.1.2272.1.29.9.1.5	8.1.60
rcRadiusSecureProfileRowStatus	1.3.6.1.4.1.2272.1.29.9.1.6	8.1.60
rcRadiusSecureProfileRootCertDestFile	1.3.6.1.4.1.2272.1.29.9.1.7	8.1.60
rcRadiusSecureProfileCertDestFile	1.3.6.1.4.1.2272.1.29.9.1.8	8.1.60
rcRadiusSecureProfileKeyDestFile	1.3.6.1.4.1.2272.1.29.9.1.9	8.1.60
rcNlsMgmtInterfaceTopologyIpFlag	1.3.6.1.4.1.2272.1.223.1.1.10	8.1.60
rcNlsMgmtTopologyIpTable	1.3.6.1.4.1.2272.1.223.11	8.1.60
rcNlsMgmtTopologyIpEntry	1.3.6.1.4.1.2272.1.223.11.1	8.1.60
rcNlsMgmtTopologyIpAddrType	1.3.6.1.4.1.2272.1.223.11.1.1	8.1.60
rcNlsMgmtTopologyIpAddr	1.3.6.1.4.1.2272.1.223.11.1.2	8.1.60
rcNlsMgmtTopologyIpInterfaceName	1.3.6.1.4.1.2272.1.223.11.1.3	8.1.60
rcNlsMgmtTopologyIpInstanceId	1.3.6.1.4.1.2272.1.223.11.1.4	8.1.60
rcNlsMgmtDhcpClient	1.3.6.1.4.1.2272.1.223.23.1	8.1.60
rcNlsMgmtIPv6AddressAddrOrigin	1.3.6.1.4.1.2272.1.223.13.1.5	8.1.60
rcNlsMgmtIPv4AddressTable	1.3.6.1.4.1.2272.1.223.12	8.1.60
rcNlsMgmtIPv4AddressEntry	1.3.6.1.4.1.2272.1.223.12.1	8.1.60
rcNlsMgmtIPv4AddressInstanceId	1.3.6.1.4.1.2272.1.223.12.1.1	8.1.60
rcNlsMgmtIPv4AddressAddress	1.3.6.1.4.1.2272.1.223.12.1.2	8.1.60
rcNlsMgmtIPv4AddressMask	1.3.6.1.4.1.2272.1.223.12.1.3	8.1.60
rcNlsMgmtIPv4AddressRowStatus	1.3.6.1.4.1.2272.1.223.12.1.4	8.1.60
rcNlsMgmtIPv4AddressAddrOrigin	1.3.6.1.4.1.2272.1.223.12.1.5	8.1.60
rcNlsMgmtIPv4AddressIntfName	1.3.6.1.4.1.2272.1.223.12.1.6	8.1.60
rcNlsMgmtIPv6AddressTable	1.3.6.1.4.1.2272.1.223.13	8.1.60
rcNlsMgmtIPv6AddressEntry	1.3.6.1.4.1.2272.1.223.13.1	8.1.60
rcNlsMgmtIPv6AddressInstanceId	1.3.6.1.4.1.2272.1.223.13.1.1	8.1.60
rcNlsMgmtIPv6AddressAddress	1.3.6.1.4.1.2272.1.223.13.1.2	8.1.60

Table continues…

Object Name	Object OID	New in VOSS Release
rcNlsMgmtIPv6AddressPrefixLength	1.3.6.1.4.1.2272.1.223.13.1.3	8.1.60
rcNlsMgmtIPv6AddressRowStatus	1.3.6.1.4.1.2272.1.223.13.1.4	8.1.60
rcNlsMgmtIPv6AddressAddrOrigin	1.3.6.1.4.1.2272.1.223.13.1.5	8.1.60
rcNlsMgmtIPv6AddressIntfName	1.3.6.1.4.1.2272.1.223.13.1.6	8.1.60
rcNlsMgmtIPv6AddressDadStatus	1.3.6.1.4.1.2272.1.223.13.1.7	8.1.60
rcSysDefaultPingTracerouteContextType	1.3.6.1.4.1.2272.1.1.126	8.1.60
rcSysDnsDomainNameOrigin	1.3.6.1.4.1.2272.1.1.128	8.1.60
rcSysDnsAdvertisedHostName	1.3.6.1.4.1.2272.1.1.129	8.1.60
rcVlanDvrGwIpv4OneIp	1.3.6.1.4.1.2272.1.3.2.1.79	8.1.60
rcVlanIsidName	1.3.6.1.4.1.2272.1.3.2.1.80	8.1.60
rcIpAdEntName	1.3.6.1.4.1.2272.1.8.2.1.13	8.1.60
rcIpAdEntIfType	1.3.6.1.4.1.2272.1.8.2.1.10	8.1.60
rcIpInterVrfStaticRouteName	1.3.6.1.4.1.2272.1.8.103.2.1.13	8.1.60
rcIpv6AddressIfType	1.3.6.1.4.1.2272.1.62.1.1.3.1.13	8.1.60
rcIpv6AddressName	1.3.6.1.4.1.2272.1.62.1.1.3.1.14	8.1.60
rcIpv6StaticRouteName	1.3.6.1.4.1.2272.1.62.1.1.6.1.10	8.1.60
rcIgmpInterfaceExtnUpnpFilterEnable	1.3.6.1.4.1.2272.1.30.1.1.38	8.1.60
rcIgmpInterfaceExtnUpnpFilterAddress	1.3.6.1.4.1.2272.1.30.1.1.39	8.1.60
rcIgmpInterfaceExtnUpnpFilterAddressMask	1.3.6.1.4.1.2272.1.30.1.1.40	8.1.60
rcNtpv4ServerHostName	1.3.6.1.4.1.2272.1.33.4.1.22	8.1.60
rcVirtualServiceVPortsPort	1.3.6.1.4.1.2272.1.101.1.1.10.1.6	8.1.60
rcVirtualServiceVPortsNicType	1.3.6.1.4.1.2272.1.101.1.1.10.1.7	8.1.60
rcVirtualServiceVPortsMacAddr	1.3.6.1.4.1.2272.1.101.1.1.10.1.8	8.1.60
rcVirtualServiceVPortsIpv4Addr	1.3.6.1.4.1.2272.1.101.1.1.10.1.9	8.1.60
rcVirtualServiceVPortsIpv6Addr	1.3.6.1.4.1.2272.1.101.1.1.10.1.10	8.1.60
rcVirtualServiceVPortsGuestIntfName	1.3.6.1.4.1.2272.1.101.1.1.10.1.11	8.1.60
rcVossSystemControlTcpKeepaliveTime	1.3.6.1.4.1.2272.1.101.1.1.1.2.2	8.1.60

Table continues…

Object Name	Object OID	New in VOSS Release
rcVossSystemControlTcpKeepaliveInterval	1.3.6.1.4.1.2272.1.101.1.1.1.2.3	8.1.60
rcVossSystemControlTcpKeepaliveProbes	1.3.6.1.4.1.2272.1.101.1.1.1.2.4	8.1.60
rcPrFilterAceIpRoutedTable	1.3.6.1.4.1.2272.1.202.1.1.2.4.40	8.1.60
rcPrFilterAceIpRoutedEntry	1.3.6.1.4.1.2272.1.202.1.1.2.4.40.1	8.1.60
rcPrFilterAceIpRoutedAclId	1.3.6.1.4.1.2272.1.202.1.1.2.4.40.1.1	8.1.60
rcPrFilterAceIpRoutedAceId	1.3.6.1.4.1.2272.1.202.1.1.2.4.40.1.2	8.1.60
rcPrFilterAceIpRoutedOnly	1.3.6.1.4.1.2272.1.202.1.1.2.4.40.1.3	8.1.60
rcPrFilterAceIpRoutedRowStatus	1.3.6.1.4.1.2272.1.202.1.1.2.4.40.1.4	8.1.60
rcPrFilterAceIpShowRoutedOnly	1.3.6.1.4.1.2272.1.202.1.1.2.4.26.1.20	8.1.60
rcPrFilterAceIpv6RoutedTable	1.3.6.1.4.1.2272.1.202.1.1.2.4.41	8.1.60
rcPrFilterAceIpv6RoutedEntry	1.3.6.1.4.1.2272.1.202.1.1.2.4.41.1	8.1.60
rcPrFilterAceIpv6RoutedAclId	1.3.6.1.4.1.2272.1.202.1.1.2.4.41.1.1	8.1.60
rcPrFilterAceIpv6RoutedAceId	1.3.6.1.4.1.2272.1.202.1.1.2.4.41.1.2	8.1.60
rcPrFilterAceIpv6RoutedOnly	1.3.6.1.4.1.2272.1.202.1.1.2.4.41.1.3	8.1.60
rcPrFilterAceIpv6RoutedRowStatus	1.3.6.1.4.1.2272.1.202.1.1.2.4.41.1.4	8.1.60
rcPrFilterAceIpv6ShowRoutedOnly	1.3.6.1.4.1.2272.1.202.1.1.2.4.32.1.13	8.1.60
rcVrfIpVpnIsidName	1.3.6.1.4.1.2272.1.203.1.1.4.1.10	8.1.60
rcIsisGlobalIpsecTunnelSourceAddress	1.3.6.1.4.1.2272.1.63.1.25	8.1.60
rcIsisLogicalInterfaceBfdEnable	1.3.6.1.4.1.2272.1.63.26.1.20	8.1.60
rcIsisLogicalInterfaceIpsecTunnelDestAddress	1.3.6.1.4.1.2272.1.63.26.1.19	8.1.60
rcIsisLogicalInterfaceEncryptionKeyLength	1.3.6.1.4.1.2272.1.63.26.1.18	8.1.60
rcIsidServiceName	1.3.6.1.4.1.2272.1.87.2.1.9	8.1.60

Table continues…

Object Name	Object OID	New in VOSS Release
rcIsidGlobalNameTable	1.3.6.1.4.1.2272.1.87.6	8.1.60
rcIsidGlobalNameEntry	1.3.6.1.4.1.2272.1.87.6.1	8.1.60
rcIsidGlobaneNameIsidId	1.3.6.1.4.1.2272.1.87.6.1.1	8.1.60
rcIsidGlobalNameIsidName	1.3.6.1.4.1.2272.1.87.6.1.2	8.1.60
rcIsidGlobalNameRowStatus	1.3.6.1.4.1.2272.1.87.6.1.3	8.1.60
rcIsidGlobalNameUsedByType	1.3.6.1.4.1.2272.1.87.6.1.4	8.1.60
rcNlsMgmtInterfaceTopologyIpFlag	1.3.6.1.4.1.2272.1.223.1.1.10	8.1.60
rcNlsMgmtZtpOn	1.3.6.1.4.1.2272.1.223.1.1.11	8.1.60
rcNlsMgmtIpStaticRouteType	1.3.6.1.4.1.2272.1.223.5.1.9	8.1.60
rcVrfIpv6IpVpnIsidName	1.3.6.1.4.1.2272.1.203.1.1.7.1.8	8.1.60
avFabricAttachZeroTouchClientAttachIsidName	1.3.6.1.4.1.45.5.46.1.29.1.7	8.2
rcnaAuthenticationFailure	1.3.6.1.4.1.2272.1.21.0.359	8.2
rcIgmpInterfaceExtnUpnpFilterEnable	1.3.6.1.4.1.2272.1.30.1.1.38	8.2
rcIgmpInterfaceExtnUpnpFilterAddress	1.3.6.1.4.1.2272.1.30.1.1.39	8.2
rcIgmpInterfaceExtnUpnpFilterAddressMask	1.3.6.1.4.1.2272.1.30.1.1.40	8.2
rcNtpv4ServerHostname	1.3.6.1.4.1.2272.1.33.4.1.22	8.2
rcVossSystemPrivExecPasswordEnable	1.3.6.1.4.1.2272.1.101.1.1.1.5	8.2
avFabricAttachIsidVlanAsgnsIsidName	1.3.6.2.4.1.45.5.46.1.5.1.7	8.2
extreme552024TVOSS	1.3.6.1.4.1.1916.2.358	8.2.5
extreme552024WVOSS	1.3.6.1.4.1.1916.2.359	8.2.5
extreme552048TVOSS	1.3.6.1.4.1.1916.2.360	8.2.5
extreme552048WVOSS	1.3.6.1.4.1.1916.2.361	8.2.5
extreme552012MW36WVOSS	1.3.6.1.4.1.1916.2.362	8.2.5
extreme552048SEVOSS	1.3.6.1.4.1.1916.2.363	8.2.5
extreme552024XVOSS	1.3.6.1.4.1.1916.2.364	8.2.5

Table 39: 5520 Series

Object Name	Object OID	New in VOSS Release
bspePethPsePortPowerClassifications	1.3.6.1.4.1.45.5.8.1.1.1.15	8.2.5
rcIpfixAgingIntervalV2	1.3.6.1.4.1.2272.1.66.1.1.5	8.2.5
rcVossSystemUBootGroup	1.3.6.1.4.1.2272.1.101.1.1.1.6	8.2.5
rcVossSystemUBootDefaultVersion	1.3.6.1.4.1.2272.1.101.1.1.1.6.1	8.2.5

Table continues…

Object Name	Object OID	New in VOSS Release
rcVossSystemUBootAlternateVersion	1.3.6.1.4.1.2272.1.101.1.1.1.6.2	8.2.5
rcVossSystemUBootVersionUsed	1.3.6.1.4.1.2272.1.101.1.1.1.6.3	8.2.5
rcVossSystemUBootTrustedDeliveryStatus	1.3.6.1.4.1.2272.1.101.1.1.1.6.4	8.2.5
rcCloudIq	1.3.6.1.4.1.2272.1.230	8.2.5
rcCloudIqObjects	1.3.6.1.4.1.2272.1.230.1	8.2.5
rcCloudIqScalars	1.3.6.1.4.1.2272.1.230.1.1	8.2.5
rcCloudIqAgentEnable	1.3.6.1.4.1.2272.1.230.1.1.1	8.2.5
rcCloudIqAgentVersion	1.3.6.1.4.1.2272.1.230.1.1.2	8.2.5
rcCloudIqServerAddressType	1.3.6.1.4.1.2272.1.230.1.1.3	8.2.5
rcCloudIqServerAddress	1.3.6.1.4.1.2272.1.230.1.1.4	8.2.5
rcCloudIqProxyAddressType	1.3.6.1.4.1.2272.1.230.1.1.5	8.2.5
rcCloudIqProxyAddress	1.3.6.1.4.1.2272.1.230.1.1.6	8.2.5
rcCloudIqProxyTcpPort	1.3.6.1.4.1.2272.1.230.1.1.7	8.2.5
rcCloudIqProxyUserName	1.3.6.1.4.1.2272.1.230.1.1.8	8.2.5
rcCloudIqProxyPassword	1.3.6.1.4.1.2272.1.230.1.1.9	8.2.5
rcCloudIqNotificationEnable	1.3.6.1.4.1.2272.1.230.1.1.10	8.2.5
rcCloudIqOperStatus	1.3.6.1.4.1.2272.1.230.1.1.11	8.2.5
rcCloudIqAssociationUrl	1.3.6.1.4.1.2272.1.230.1.1.12	8.2.5
rcCloudIqPollUrl	1.3.6.1.4.1.2272.1.230.1.1.13	8.2.5
rcCloudIqMonitorFreq	1.3.6.1.4.1.2272.1.230.1.1.14	8.2.5
rcCloudIqPollFreq	1.3.6.1.4.1.2272.1.230.1.1.15	8.2.5
rcCloudIqLastOnboardTime	1.3.6.1.4.1.2272.1.230.1.1.16	8.2.5
rcCloudIqLastPollStatus	1.3.6.1.4.1.2272.1.230.1.1.17	8.2.5
rcCloudIqLastPollTime	1.3.6.1.4.1.2272.1.230.1.1.18	8.2.5
rcCloudIqLastMonitorStatus	1.3.6.1.4.1.2272.1.230.1.1.19	8.2.5
rcCloudIqLastMonitorTime	1.3.6.1.4.1.2272.1.230.1.1.20	8.2.5
rcCloudIqLastHealthStatus	1.3.6.1.4.1.2272.1.230.1.1.21	8.2.5
rcCloudIqLastHealthTime	1.3.6.1.4.1.2272.1.230.1.1.22	8.2.5
rcnCloudIqUpTrap	1.3.6.1.4.1.2272.1.21.0.357	8.2.5
rcnCloudIqDownTrap	1.3.6.1.4.1.2272.1.21.0.358	8.2.5

Table 40: VSP 4900 Series

Object Name	Object OID	New in VOSS Release
rcCloudIq	1.3.6.1.4.1.2272.1.230	8.1.1

Table continues…

Object Name	Object OID	New in VOSS Release
rcCloudIqObjects	1.3.6.1.4.1.2272.1.230.1	8.1.1
rcCloudIqScalars	1.3.6.1.4.1.2272.1.230.1.1	8.1.1
rcCloudIqAgentEnable	1.3.6.1.4.1.2272.1.230.1.1.1	8.1.1
rcCloudIqAgentVersion	1.3.6.1.4.1.2272.1.230.1.1.2	8.1.1
rcCloudIqServerAddressType	1.3.6.1.4.1.2272.1.230.1.1.3	8.1.1
rcCloudIqServerAddress	1.3.6.1.4.1.2272.1.230.1.1.4	8.1.1
rcCloudIqProxyAddressType	1.3.6.1.4.1.2272.1.230.1.1.5	8.1.1
rcCloudIqProxyAddress	1.3.6.1.4.1.2272.1.230.1.1.6	8.1.1
rcCloudIqProxyTcpPort	1.3.6.1.4.1.2272.1.230.1.1.7	8.1.1
rcCloudIqProxyUserName	1.3.6.1.4.1.2272.1.230.1.1.8	8.1.1
rcCloudIqProxyPassword	1.3.6.1.4.1.2272.1.230.1.1.9	8.1.1
rcCloudIqNotificationEnable	1.3.6.1.4.1.2272.1.230.1.1.10	8.1.1
rcCloudIqOperStatus	1.3.6.1.4.1.2272.1.230.1.1.11	8.1.1
rcCloudIqAssociationUrl	1.3.6.1.4.1.2272.1.230.1.1.12	8.1.1
rcCloudIqPollUrl	1.3.6.1.4.1.2272.1.230.1.1.13	8.1.1
rcCloudIqMonitorFreq	1.3.6.1.4.1.2272.1.230.1.1.14	8.1.1
rcCloudIqPollFreq	1.3.6.1.4.1.2272.1.230.1.1.15	8.1.1
rcCloudIqLastOnboardTime	1.3.6.1.4.1.2272.1.230.1.1.16	8.1.1
rcCloudIqLastPollStatus	1.3.6.1.4.1.2272.1.230.1.1.17	8.1.1
rcCloudIqLastPollTime	1.3.6.1.4.1.2272.1.230.1.1.18	8.1.1
rcCloudIqLastMonitorStatus	1.3.6.1.4.1.2272.1.230.1.1.19	8.1.1
rcCloudIqLastMonitorTime	1.3.6.1.4.1.2272.1.230.1.1.20	8.1.1
rcCloudIqLastHealthStatus	1.3.6.1.4.1.2272.1.230.1.1.21	8.1.1
rcCloudIqLastHealthTime	1.3.6.1.4.1.2272.1.230.1.1.22	8.1.1
rcnCloudIqUpTrap	1.3.6.1.4.1.2272.1.21.0.357	8.1.1
rcnCloudIqDownTrap	1.3.6.1.4.1.2272.1.21.0.358	8.1.1
rcVossSystemSsdInfoGroup	1.3.6.1.4.1.2272.1.101.1.1.1.4	8.1.5
bspePethMainPseFastPoeEnable	1.3.6.1.4.1.45.5.8.1.2.1.4	8.2
bspePethMainPsePerpetualPoeEnable	1.3.6.1.4.1.45.5.8.1.2.1.5	8.2
bspePethPsePortExtFastPoeEnable	1.3.6.1.4.1.45.5.8.1.1.1.13	8.2
bspePethPsePortExtPerpetualPoeEnable	1.3.6.1.4.1.45.5.8.1.1.1.14	8.2
rcSysDnsDomainNameOrigin	1.3.6.1.4.1.2272.1.1.128	8.2
rcSysDnsAdvertisedHostName	1.3.6.1.4.1.2272.1.1.129	8.2

Table continues…

Object Name	Object OID	New in VOSS Release
rcVlanIsidName	1.3.6.1.4.1.2272.1.3.2.1.80	8.2
rcIpAdEntName	1.3.6.1.4.1.2272.1.8.2.1.13	8.2
rcIpStaticRouteName	1.3.6.1.4.1.2272.1.8.15.2.1.11	8.2
rcIgmpStreamTimeout	1.3.6.1.4.1.2272.1.30.11.7.0	8.2
rcIpv6StaticRouteName	1.3.6.1.4.1.2272.1.62.1.1.6.1.10	8.2
rcIsisGlobalMgmtClipIpAddr	1.3.6.1.4.1.2272.1.63.1.26	8.2
rcIsisLogicalInterfaceBfdEnable	1.3.6.1.4.1.2272.1.63.26.1.20	8.2
rcIsidGlobalNameTable	1.3.6.1.4.1.2272.1.87.6	8.2
rcPrFilterAceIpShowRoutedOnly	1.3.6.1.4.1.2272.1.202.1.1.2.4.26.1.20	8.2
rcPrFilterAceIpv6ShowRoutedOnly	1.3.6.1.4.1.2272.1.202.1.1.2.4.32.1.13	8.2
rcPrFilterAceIpRoutedTable	1.3.6.1.4.1.2272.1.202.1.1.2.4.40	8.2
rcPrFilterAceIpv6RoutedTable	1.3.6.1.4.1.2272.1.202.1.1.2.4.41	8.2
rcVrfIpVpnIsidName	1.3.6.1.4.1.2272.1.203.1.1.4.1.10	8.2
rcVrfIpv6IpVpnIsidName	1.3.6.1.4.1.2272.1.203.1.1.7.1.8	8.2
rcIsidServiceName	1.3.6.1.4.2272.1.87.2.1.8	8.2

Table 41: VSP 7200 Series

Object Name	Object OID	New in VOSS Release
rcEndpointTrackingAutoIsidOffset	1.3.6.1.4.1.2272.1.228.1.1.1.1	8.1
rcEndpointTrackingAutoIsidOffsetEnable	1.3.6.1.4.1.2272.1.228.1.1.1.2	8.1
rcEndpointTrackingGlobalEnable	1.3.6.1.4.1.2272.1.228.1.1.1.3	8.1
rcEndpointTrackingInterfaceTable	1.3.6.1.4.1.2272.1.228.1.1.2	8.1
rcEndpointTrackingInterfaceEntry	1.3.6.1.4.1.2272.1.228.1.1.2.1	8.1
rcEndpointTrackingInterfaceIndex	1.3.6.1.4.1.2272.1.228.1.1.2.1.1	8.1
rcEndpointTrackingInterfaceEnable	1.3.6.1.4.1.2272.1.228.1.1.2.1.2	8.1
rcEndpointTrackingInterfaceRowStatus	1.3.6.1.4.1.2272.1.228.1.1.2.1.3	8.1
rcEndpointTrackingBindingTable	1.3.6.1.4.1.2272.1.228.1.1.3	8.1

Table continues…

Object Name	Object OID	New in VOSS Release
rcEndpointTrackingBindingEntry	1.3.6.1.4.1.2272.1.228.1.1.3.1	8.1
rcEndpointTrackingBindingIfIndex	1.3.6.1.4.1.2272.1.228.1.1.3.1.1	8.1
rcEndpointTrackingBindingMacAddr	1.3.6.1.4.1.2272.1.228.1.1.3.1.2	8.1
rcEndpointTrackingBindingStatus	1.3.6.1.4.1.2272.1.228.1.1.3.1.3	8.1
rcEndpointTrackingBindingVlanId	1.3.6.1.4.1.2272.1.228.1.1.3.1.4	8.1
rcEndpointTrackingBindingIsid	1.3.6.1.4.1.2272.1.228.1.1.3.1.5	8.1
rcEndpointTrackingBindingIsidSource	1.3.6.1.4.1.2272.1.228.1.1.3.1.6	8.1
rcEndpointTrackingBindingTimeout	1.3.6.1.4.1.2272.1.228.1.1.3.1.7	8.1
rcEndpointTrackingBindingTimeRemaining	1.3.6.1.4.1.2272.1.228.1.1.3.1.8	8.1
rcSysDnsDomainNameOrigin	1.3.6.1.4.1.2272.1.1.128	8.2
rcSysDnsAdvertisedHostName	1.3.6.1.4.1.2272.1.1.129	8.2
rcVlanIsidName	1.3.6.1.4.1.2272.1.3.2.1.80	8.2
rcIpAdEntName	1.3.6.1.4.1.2272.1.8.2.1.13	8.2
rcIpStaticRouteName	1.3.6.1.4.1.2272.1.8.15.2.1.11	8.2
rcnCloudIqUpTrap	1.3.6.1.4.1.2272.1.21.0.357	8.2
rcnCloudIqDownTrap	1.3.6.1.4.1.2272.1.21.0.358	8.2
rcIgmpStreamTimeout	1.3.6.1.4.1.2272.1.30.11.7.0	8.2
rcIpv6StaticRouteName	1.3.6.1.4.1.2272.1.62.1.1.6.1.10	8.2
rcIsisGlobalMgmtClipIpAddr	1.3.6.1.4.1.2272.1.63.1.26	8.2
rcIsisLogicalInterfaceBfdEnable	1.3.6.1.4.1.2272.1.63.26.1.20	8.2
rcIsidGlobalNameTable	1.3.6.1.4.1.2272.1.87.6	8.2
rcPrFilterAceIpShowRoutedOnly	1.3.6.1.4.1.2272.1.202.1.1.2.4.26.1.20	8.2
rcPrFilterAceIpv6ShowRoutedOnly	1.3.6.1.4.1.2272.1.202.1.1.2.4.32.1.13	8.2
rcPrFilterAceIpRoutedTable	1.3.6.1.4.1.2272.1.202.1.1.2.4.40	8.2

Table continues…

Object Name	Object OID	New in VOSS Release
rcPrFilterAceIpv6RoutedTable	1.3.6.1.4.1.2272.1.202.1.1.2.4.41	8.2
rcVrfIpVpnIsidName	1.3.6.1.4.1.2272.1.203.1.1.4.1.10	8.2
rcVrfIpv6IpVpnIsidName	1.3.6.1.4.1.2272.1.203.1.1.7.1.8	8.2
rcIsidServiceName	1.3.6.1.4.2272.1.87.2.1.8	8.2
rcCloudIq	1.3.6.1.4.1.2272.1.230	8.2
rcCloudIqObjects	1.3.6.1.4.1.2272.1.230.1	8.2
rcCloudIqScalars	1.3.6.1.4.1.2272.1.230.1.1	8.2
rcCloudIqAgentEnable	1.3.6.1.4.1.2272.1.230.1.1.1	8.2
rcCloudIqAgentVersion	1.3.6.1.4.1.2272.1.230.1.1.2	8.2
rcCloudIqServerAddressType	1.3.6.1.4.1.2272.1.230.1.1.3	8.2
rcCloudIqServerAddress	1.3.6.1.4.1.2272.1.230.1.1.4	8.2
rcCloudIqProxyAddressType	1.3.6.1.4.1.2272.1.230.1.1.5	8.2
rcCloudIqProxyAddress	1.3.6.1.4.1.2272.1.230.1.1.6	8.2
rcCloudIqProxyTcpPort	1.3.6.1.4.1.2272.1.230.1.1.7	8.2
rcCloudIqProxyUserName	1.3.6.1.4.1.2272.1.230.1.1.8	8.2
rcCloudIqProxyPassword	1.3.6.1.4.1.2272.1.230.1.1.9	8.2
rcCloudIqNotificationEnable	1.3.6.1.4.1.2272.1.230.1.1.10	8.2
rcCloudIqOperStatus	1.3.6.1.4.1.2272.1.230.1.1.11	8.2
rcCloudIqAssociationUrl	1.3.6.1.4.1.2272.1.230.1.1.12	8.2
rcCloudIqPollUrl	1.3.6.1.4.1.2272.1.230.1.1.13	8.2
rcCloudIqMonitorFreq	1.3.6.1.4.1.2272.1.230.1.1.14	8.2
rcCloudIqPollFreq	1.3.6.1.4.1.2272.1.230.1.1.15	8.2
rcCloudIqLastOnboardTime	1.3.6.1.4.1.2272.1.230.1.1.16	8.2
rcCloudIqLastPollStatus	1.3.6.1.4.1.2272.1.230.1.1.17	8.2
rcCloudIqLastPollTime	1.3.6.1.4.1.2272.1.230.1.1.18	8.2
rcCloudIqLastMonitorStatus	1.3.6.1.4.1.2272.1.230.1.1.19	8.2
rcCloudIqLastMonitorTime	1.3.6.1.4.1.2272.1.230.1.1.20	8.2
rcCloudIqLastHealthStatus	1.3.6.1.4.1.2272.1.230.1.1.21	8.2
rcCloudIqLastHealthTime	1.3.6.1.4.1.2272.1.230.1.1.22	8.2
rcCloudIqServerAddressOrigin	1.3.6.1.4.1.2272.1.230.1.1.23	8.2

Table 42: VSP 7400 Series

Object Name	Object OID	New in VOSS Release
rcEndpointTrackingAutoIsidOffset	1.3.6.1.4.1.2272.1.228.1.1.1.1	8.1
rcEndpointTrackingAutoIsidOffsetEnable	1.3.6.1.4.1.2272.1.228.1.1.1.2	8.1
rcEndpointTrackingGlobalEnable	1.3.6.1.4.1.2272.1.228.1.1.1.3	8.1
rcEndpointTrackingInterfaceTable	1.3.6.1.4.1.2272.1.228.1.1.2	8.1
rcEndpointTrackingInterfaceEntry	1.3.6.1.4.1.2272.1.228.1.1.2.1	8.1
rcEndpointTrackingInterfaceIndex	1.3.6.1.4.1.2272.1.228.1.1.2.1.1	8.1
rcEndpointTrackingInterfaceEnable	1.3.6.1.4.1.2272.1.228.1.1.2.1.2	8.1
rcEndpointTrackingInterfaceRowStatus	1.3.6.1.4.1.2272.1.228.1.1.2.1.3	8.1
rcEndpointTrackingBindingTable	1.3.6.1.4.1.2272.1.228.1.1.3	8.1
rcEndpointTrackingBindingEntry	1.3.6.1.4.1.2272.1.228.1.1.3.1	8.1
rcEndpointTrackingBindingIfIndex	1.3.6.1.4.1.2272.1.228.1.1.3.1.1	8.1
rcEndpointTrackingBindingMacAddr	1.3.6.1.4.1.2272.1.228.1.1.3.1.2	8.1
rcEndpointTrackingBindingStatus	1.3.6.1.4.1.2272.1.228.1.1.3.1.3	8.1
rcEndpointTrackingBindingVlanId	1.3.6.1.4.1.2272.1.228.1.1.3.1.4	8.1
rcEndpointTrackingBindingIsid	1.3.6.1.4.1.2272.1.228.1.1.3.1.5	8.1
rcEndpointTrackingBindingIsidSource	1.3.6.1.4.1.2272.1.228.1.1.3.1.6	8.1
rcEndpointTrackingBindingTimeout	1.3.6.1.4.1.2272.1.228.1.1.3.1.7	8.1
rcEndpointTrackingBindingTimeRemaining	1.3.6.1.4.1.2272.1.228.1.1.3.1.8	8.1
rcCloudIq	1.3.6.1.4.1.2272.1.230	8.1.1
rcCloudIqObjects	1.3.6.1.4.1.2272.1.230.1	8.1.1
rcCloudIqScalars	1.3.6.1.4.1.2272.1.230.1.1	8.1.1
rcCloudIqAgentEnable	1.3.6.1.4.1.2272.1.230.1.1.1	8.1.1

Table continues…

Object Name	Object OID	New in VOSS Release
rcCloudIqAgentVersion	1.3.6.1.4.1.2272.1.230.1.1.2	8.1.1
rcCloudIqServerAddressType	1.3.6.1.4.1.2272.1.230.1.1.3	8.1.1
rcCloudIqServerAddress	1.3.6.1.4.1.2272.1.230.1.1.4	8.1.1
rcCloudIqProxyAddressType	1.3.6.1.4.1.2272.1.230.1.1.5	8.1.1
rcCloudIqProxyAddress	1.3.6.1.4.1.2272.1.230.1.1.6	8.1.1
rcCloudIqProxyTcpPort	1.3.6.1.4.1.2272.1.230.1.1.7	8.1.1
rcCloudIqProxyUserName	1.3.6.1.4.1.2272.1.230.1.1.8	8.1.1
rcCloudIqProxyPassword	1.3.6.1.4.1.2272.1.230.1.1.9	8.1.1
rcCloudIqNotificationEnable	1.3.6.1.4.1.2272.1.230.1.1.10	8.1.1
rcCloudIqOperStatus	1.3.6.1.4.1.2272.1.230.1.1.11	8.1.1
rcCloudIqAssociationUrl	1.3.6.1.4.1.2272.1.230.1.1.12	8.1.1
rcCloudIqPollUrl	1.3.6.1.4.1.2272.1.230.1.1.13	8.1.1
rcCloudIqMonitorFreq	1.3.6.1.4.1.2272.1.230.1.1.14	8.1.1
rcCloudIqPollFreq	1.3.6.1.4.1.2272.1.230.1.1.15	8.1.1
rcCloudIqLastOnboardTime	1.3.6.1.4.1.2272.1.230.1.1.16	8.1.1
rcCloudIqLastPollStatus	1.3.6.1.4.1.2272.1.230.1.1.17	8.1.1
rcCloudIqLastPollTime	1.3.6.1.4.1.2272.1.230.1.1.18	8.1.1
rcCloudIqLastMonitorStatus	1.3.6.1.4.1.2272.1.230.1.1.19	8.1.1
rcCloudIqLastMonitorTime	1.3.6.1.4.1.2272.1.230.1.1.20	8.1.1
rcCloudIqLastHealthStatus	1.3.6.1.4.1.2272.1.230.1.1.21	8.1.1
rcCloudIqLastHealthTime	1.3.6.1.4.1.2272.1.230.1.1.22	8.1.1
rcnCloudIqUpTrap	1.3.6.1.4.1.2272.1.21.0.357	8.1.1
rcnCloudIqDownTrap	1.3.6.1.4.1.2272.1.21.0.358	8.1.1
rcSysDnsDomainNameOrigin	1.3.6.1.4.1.2272.1.1.128	8.2
rcSysDnsAdvertisedHostName	1.3.6.1.4.1.2272.1.1.129	8.2
rcVlanIsidName	1.3.6.1.4.1.2272.1.3.2.1.80	8.2
rcIpAdEntName	1.3.6.1.4.1.2272.1.8.2.1.13	8.2
rcIpStaticRouteName	1.3.6.1.4.1.2272.1.8.15.2.1.11	8.2
rcIgmpStreamTimeout	1.3.6.1.4.1.2272.1.30.11.7.0	8.2
rcIpv6StaticRouteName	1.3.6.1.4.1.2272.1.62.1.1.6.1.10	8.2
rcIsisGlobalMgmtClipIpAddr	1.3.6.1.4.1.2272.1.63.1.26	8.2
rcIsisLogicalInterfaceBfdEnable	1.3.6.1.4.1.2272.1.63.26.1.20	8.2
rcIsidGlobalNameTable	1.3.6.1.4.1.2272.1.87.6	8.2

Table continues…

Object Name	Object OID	New in VOSS Release
rcPrFilterAceIpShowRoutedOnly	1.3.6.1.4.1.2272.1.202.1.1.2.4.26.1.20	8.2
rcPrFilterAceIpv6ShowRoutedOnly	1.3.6.1.4.1.2272.1.202.1.1.2.4.32.1.13	8.2
rcPrFilterAceIpRoutedTable	1.3.6.1.4.1.2272.1.202.1.1.2.4.40	8.2
rcPrFilterAceIpv6RoutedTable	1.3.6.1.4.1.2272.1.202.1.1.2.4.41	8.2
rcVrfIpVpnIsidName	1.3.6.1.4.1.2272.1.203.1.1.4.1.10	8.2
rcVrfIpv6IpVpnIsidName	1.3.6.1.4.1.2272.1.203.1.1.7.1.8	8.2
rcIsidServiceName	1.3.6.1.4.2272.1.87.2.1.8	8.2

Table 43: VSP 8000 Series

Object Name	Object OID	New in VOSS Release
rcPortMacsecMKAProfileName	1.3.6.1.4.1.2272.1.4.10.1.1.127	8.1
rcMACSecMKAProfileTable	1.3.6.1.4.1.2272.1.88.3	8.1
rcMACSecMKAProfileEntry	1.3.6.1.4.1.2272.1.88.3.1	8.1
rcMACSecMKAProfileId	1.3.6.1.4.1.2272.1.88.3.1.1	8.1
rcMACSecMKAProfileName	1.3.6.1.4.1.2272.1.88.3.1.2	8.1
rcMACSecMKAProfileReplayProtectEnable	1.3.6.1.4.1.2272.1.88.3.1.3	8.1
rcMACSecMKAProfileReplayProtectWindow	1.3.6.1.4.1.2272.1.88.3.1.4	8.1
rcMACSecMKAProfileOffsetValue	1.3.6.1.4.1.2272.1.88.3.1.5	8.1
rcMACSecMKAProfileRowStatus	1.3.6.1.4.1.2272.1.88.3.1.6	8.1
rcMACSecMKAProfilePortMembers	1.3.6.1.4.1.2272.1.88.3.1.7	8.1
rcMACSecMKAProfileCipherSuite	1.3.6.1.4.1.2272.1.88.3.1.8	8.1
rcMACSecMKAStatsTable	1.3.6.1.4.1.2272.1.88.4	8.1
rcMACSecMKAStatsEntry	1.3.6.1.4.1.2272.1.88.4.1	8.1
rcMACSecMKAMKPDUValidatedPkts	1.3.6.1.4.1.2272.1.88.4.1.1	8.1
rcMACSecMKARxDistributedSAKPkts	1.3.6.1.4.1.2272.1.88.4.1.2	8.1
rcMACSecMKAMKPDUTransmittedPkts	1.3.6.1.4.1.2272.1.88.4.1.3	8.1
rcMACSecMKATxDistributedSAKPkts	1.3.6.1.4.1.2272.1.88.4.1.4	8.1
rcMACSecMKAClearStats	1.3.6.1.4.1.2272.1.88.4.1.5	8.1

Table continues…

Object Name	Object OID	New in VOSS Release
rcEndpointTrackingAutoIsidOffset	1.3.6.1.4.1.2272.1.228.1.1.1.1	8.1
rcEndpointTrackingAutoIsidOffsetEnable	1.3.6.1.4.1.2272.1.228.1.1.1.2	8.1
rcEndpointTrackingGlobalEnable	1.3.6.1.4.1.2272.1.228.1.1.1.3	8.1
rcEndpointTrackingInterfaceTable	1.3.6.1.4.1.2272.1.228.1.1.2	8.1
rcEndpointTrackingInterfaceEntry	1.3.6.1.4.1.2272.1.228.1.1.2.1	8.1
rcEndpointTrackingInterfaceIndex	1.3.6.1.4.1.2272.1.228.1.1.2.1.1	8.1
rcEndpointTrackingInterfaceEnable	1.3.6.1.4.1.2272.1.228.1.1.2.1.2	8.1
rcEndpointTrackingInterfaceRowStatus	1.3.6.1.4.1.2272.1.228.1.1.2.1.3	8.1
rcEndpointTrackingBindingTable	1.3.6.1.4.1.2272.1.228.1.1.3	8.1
rcEndpointTrackingBindingEntry	1.3.6.1.4.1.2272.1.228.1.1.3.1	8.1
rcEndpointTrackingBindingIfIndex	1.3.6.1.4.1.2272.1.228.1.1.3.1.1	8.1
rcEndpointTrackingBindingMacAddr	1.3.6.1.4.1.2272.1.228.1.1.3.1.2	8.1
rcEndpointTrackingBindingStatus	1.3.6.1.4.1.2272.1.228.1.1.3.1.3	8.1
rcEndpointTrackingBindingVlanId	1.3.6.1.4.1.2272.1.228.1.1.3.1.4	8.1
rcEndpointTrackingBindingIsid	1.3.6.1.4.1.2272.1.228.1.1.3.1.5	8.1
rcEndpointTrackingBindingIsidSource	1.3.6.1.4.1.2272.1.228.1.1.3.1.6	8.1
rcEndpointTrackingBindingTimeout	1.3.6.1.4.1.2272.1.228.1.1.3.1.7	8.1
rcEndpointTrackingBindingTimeRemaining	1.3.6.1.4.1.2272.1.228.1.1.3.1.8	8.1
ieee8021XPaeKaY	1.3.111.2.802.1.1.15.1.6	8.1
ieee8021XKayMkaTable	1.3.111.2.802.1.1.15.1.6.1	8.1
ieee8021XKayMkaEntry	1.3.111.2.802.1.1.15.1.6.1.1	8.1
ieee8021XKayMkaActive	1.3.111.2.802.1.1.15.1.6.1.1.1	8.1
ieee8021XKayMkaAuthenticated	1.3.111.2.802.1.1.15.1.6.1.1.2	8.1

Table continues…

Object Name	Object OID	New in VOSS Release
ieee8021XKayMkaSecured	1.3.111.2.802.1.1.15.1.6.1.1.3	8.1
ieee8021XKayMkaFailed	1.3.111.2.802.1.1.15.1.6.1.1.4	8.1
ieee8021XKayMkaActorSCI	1.3.111.2.802.1.1.15.1.6.1.1.5	8.1
ieee8021XKayMkaActorsPriority	1.3.111.2.802.1.1.15.1.6.1.1.6	8.1
ieee8021XKayMkaKeyServerPriority	1.3.111.2.802.1.1.15.1.6.1.1.7	8.1
ieee8021XKayMkaKeyServerSCI	1.3.111.2.802.1.1.15.1.6.1.1.8	8.1
ieee8021XKayAllowedJoinGroup	1.3.111.2.802.1.1.15.1.6.1.1.9	8.1
ieee8021XKayAllowedFormGroup	1.3.111.2.802.1.1.15.1.6.1.1.10	8.1
ieee8021XKayCreateNewGroup	1.3.111.2.802.1.1.15.1.6.1.1.11	8.1
ieee8021XKayMacSecCapability	1.3.111.2.802.1.1.15.1.6.1.1.12	8.1
ieee8021XKayMacSecDesired	1.3.111.2.802.1.1.15.1.6.1.1.13	8.1
ieee8021XKayMacSecProtect	1.3.111.2.802.1.1.15.1.6.1.1.14	8.1
ieee8021XKayMacSecReplayProtect	1.3.111.2.802.1.1.15.1.6.1.1.15	8.1
ieee8021XKayMacSecValidate	1.3.111.2.802.1.1.15.1.6.1.1.16	8.1
ieee8021XKayMacSecConfidentialityOffset	1.3.111.2.802.1.1.15.1.6.1.1.17	8.1
ieee8021XKayMkaTxKN	1.3.111.2.802.1.1.15.1.6.1.1.18	8.1
ieee8021XKayMkaTxAN	1.3.111.2.802.1.1.15.1.6.1.1.19	8.1
ieee8021XKayMkaRxKN	1.3.111.2.802.1.1.15.1.6.1.1.20	8.1
ieee8021XKayMkaRxAN	1.3.111.2.802.1.1.15.1.6.1.1.21	8.1
ieee8021XKayMkaParticipantTable	1.3.111.2.802.1.1.15.1.6.2	8.1
Ieee8021XKayMkaParticipantEntry	1.3.111.2.802.1.1.15.1.6.2.1	8.1
ieee8021XKayMkaPartCKN	1.3.111.2.802.1.1.15.1.6.2.1.1	8.1
ieee8021XKayMkaPartKMD	1.3.111.2.802.1.1.15.1.6.2.1.2	8.1
ieee8021XKayMkaPartNID	1.3.111.2.802.1.1.15.1.6.2.1.3	8.1
ieee8021XKayMkaPartCached	1.3.111.2.802.1.1.15.1.6.2.1.4	8.1
ieee8021XKayMkaPartActive	1.3.111.2.802.1.1.15.1.6.2.1.5	8.1

Table continues…

Object Name	Object OID	New in VOSS Release
ieee8021XKayMkaPartRetain	1.3.111.2.802.1.1.15.1.6.2.1.6	8.1
ieee8021XKayMkaPartActivateControl	1.3.111.2.802.1.1.15.1.6.2.1.7	8.1
ieee8021XKayMkaPartPrincipal	1.3.111.2.802.1.1.15.1.6.2.1.8	8.1
ieee8021XKayMkaPartDistCKN	1.3.111.2.802.1.1.15.1.6.2.1.9	8.1
ieee8021XKayMkaPartRowStatus	1.3.111.2.802.1.1.15.1.6.2.1.10	8.1
ieee8021XKayMkaPeerListTable	1.3.111.2.802.1.1.15.1.6.3	8.1
Ieee8021XKayMkaPeerListEntry	1.3.111.2.802.1.1.15.1.6.3.1	8.1
ieee8021XKayMkaPeerListMI	1.3.111.2.802.1.1.15.1.6.3.1.1	8.1
ieee8021XKayMkaPeerListMN	1.3.111.2.802.1.1.15.1.6.3.1.2	8.1
ieee8021XKayMkaPeerListType	1.3.111.2.802.1.1.15.1.6.3.1.3	8.1
ieee8021XKayMkaPeerListSCI	1.3.111.2.802.1.1.15.1.6.3.1.4	8.1
rcSysDnsDomainNameOrigin	1.3.6.1.4.1.2272.1.1.128	8.2
rcSysDnsAdvertisedHostName	1.3.6.1.4.1.2272.1.1.129	8.2
rcVlanIsidName	1.3.6.1.4.1.2272.1.3.2.1.80	8.2
rcIpAdEntName	1.3.6.1.4.1.2272.1.8.2.1.13	8.2
rcIpStaticRouteName	1.3.6.1.4.1.2272.1.8.15.2.1.11	8.2
rcnCloudIqUpTrap	1.3.6.1.4.1.2272.1.21.0.357	8.2
rcnCloudIqDownTrap	1.3.6.1.4.1.2272.1.21.0.358	8.2
rcIgmpStreamTimeout	1.3.6.1.4.1.2272.1.30.11.7.0	8.2
rcIpv6StaticRouteName	1.3.6.1.4.1.2272.1.62.1.1.6.1.10	8.2
rcIsisGlobalMgmtClipIpAddr	1.3.6.1.4.1.2272.1.63.1.26	8.2
rcIsisLogicalInterfaceBfdEnable	1.3.6.1.4.1.2272.1.63.26.1.20	8.2
rcIsidGlobalNameTable	1.3.6.1.4.1.2272.1.87.6	8.2
rcVrfIpVpnIsidName	1.3.6.1.4.1.2272.1.203.1.1.4.1.10	8.2
rcPrFilterAceIpShowRoutedOnly	1.3.6.1.4.1.2272.1.202.1.1.2.4.26.1.20	8.2
rcPrFilterAceIpv6ShowRoutedOnly	1.3.6.1.4.1.2272.1.202.1.1.2.4.32.1.13	8.2
rcPrFilterAceIpRoutedTable	1.3.6.1.4.1.2272.1.202.1.1.2.4.40	8.2
rcPrFilterAceIpv6RoutedTable	1.3.6.1.4.1.2272.1.202.1.1.2.4.41	8.2
rcVrfIpv6IpVpnIsidName	1.3.6.1.4.1.2272.1.203.1.1.7.1.8	8.2

Table continues…

Object Name	Object OID	New in VOSS Release
rcIsidServiceName	1.3.6.1.4.2272.1.87.2.1.8	8.2
rcCloudIq	1.3.6.1.4.1.2272.1.230	8.2
rcCloudIqObjects	1.3.6.1.4.1.2272.1.230.1	8.2
rcCloudIqScalars	1.3.6.1.4.1.2272.1.230.1.1	8.2
rcCloudIqAgentEnable	1.3.6.1.4.1.2272.1.230.1.1.1	8.2
rcCloudIqAgentVersion	1.3.6.1.4.1.2272.1.230.1.1.2	8.2
rcCloudIqServerAddressType	1.3.6.1.4.1.2272.1.230.1.1.3	8.2
rcCloudIqServerAddress	1.3.6.1.4.1.2272.1.230.1.1.4	8.2
rcCloudIqProxyAddressType	1.3.6.1.4.1.2272.1.230.1.1.5	8.2
rcCloudIqProxyAddress	1.3.6.1.4.1.2272.1.230.1.1.6	8.2
rcCloudIqProxyTcpPort	1.3.6.1.4.1.2272.1.230.1.1.7	8.2
rcCloudIqProxyUserName	1.3.6.1.4.1.2272.1.230.1.1.8	8.2
rcCloudIqProxyPassword	1.3.6.1.4.1.2272.1.230.1.1.9	8.2
rcCloudIqNotificationEnable	1.3.6.1.4.1.2272.1.230.1.1.10	8.2
rcCloudIqOperStatus	1.3.6.1.4.1.2272.1.230.1.1.11	8.2
rcCloudIqAssociationUrl	1.3.6.1.4.1.2272.1.230.1.1.12	8.2
rcCloudIqPollUrl	1.3.6.1.4.1.2272.1.230.1.1.13	8.2
rcCloudIqMonitorFreq	1.3.6.1.4.1.2272.1.230.1.1.14	8.2
rcCloudIqPollFreq	1.3.6.1.4.1.2272.1.230.1.1.15	8.2
rcCloudIqLastOnboardTime	1.3.6.1.4.1.2272.1.230.1.1.16	8.2
rcCloudIqLastPollStatus	1.3.6.1.4.1.2272.1.230.1.1.17	8.2
rcCloudIqLastPollTime	1.3.6.1.4.1.2272.1.230.1.1.18	8.2
rcCloudIqLastMonitorStatus	1.3.6.1.4.1.2272.1.230.1.1.19	8.2
rcCloudIqLastMonitorTime	1.3.6.1.4.1.2272.1.230.1.1.20	8.2
rcCloudIqLastHealthStatus	1.3.6.1.4.1.2272.1.230.1.1.21	8.2
rcCloudIqLastHealthTime	1.3.6.1.4.1.2272.1.230.1.1.22	8.2

Table 44: XA1400 Series

Object Name	Object OID	New in VOSS Release
rcNlsMgmtInterfaceTable	1.3.6.1.4.1.2272.1.223.1	8.1.1
rcNlsMgmtAddressTable	1.3.6.1.4.1.2272.1.223.2	8.1.1
rcNlsMgmtIpArpTable	1.3.6.1.4.1.2272.1.223.3	8.1.1
rcNlsMgmtIpStaticRouteTable	1.3.6.1.4.1.2272.1.223.5	8.1.1
rcNlsMgmtStatsTable	1.3.6.1.4.1.2272.1.223.7	8.1.1
rcNlsMgmtIpRouteTable	1.3.6.1.4.1.2272.1.223.8	8.1.1

Table continues…

Object Name	Object OID	New in VOSS Release
rcCloudIq	1.3.6.1.4.1.2272.1.230	8.1.1
rcCloudIqObjects	1.3.6.1.4.1.2272.1.230.1	8.1.1
rcCloudIqScalars	1.3.6.1.4.1.2272.1.230.1.1	8.1.1
rcCloudIqAgentEnable	1.3.6.1.4.1.2272.1.230.1.1.1	8.1.1
rcCloudIqAgentVersion	1.3.6.1.4.1.2272.1.230.1.1.2	8.1.1
rcCloudIqServerAddressType	1.3.6.1.4.1.2272.1.230.1.1.3	8.1.1
rcCloudIqServerAddress	1.3.6.1.4.1.2272.1.230.1.1.4	8.1.1
rcCloudIqProxyAddressType	1.3.6.1.4.1.2272.1.230.1.1.5	8.1.1
rcCloudIqProxyAddress	1.3.6.1.4.1.2272.1.230.1.1.6	8.1.1
rcCloudIqProxyTcpPort	1.3.6.1.4.1.2272.1.230.1.1.7	8.1.1
rcCloudIqProxyUserName	1.3.6.1.4.1.2272.1.230.1.1.8	8.1.1
rcCloudIqProxyPassword	1.3.6.1.4.1.2272.1.230.1.1.9	8.1.1
rcCloudIqNotificationEnable	1.3.6.1.4.1.2272.1.230.1.1.10	8.1.1
rcCloudIqOperStatus	1.3.6.1.4.1.2272.1.230.1.1.11	8.1.1
rcCloudIqAssociationUrl	1.3.6.1.4.1.2272.1.230.1.1.12	8.1.1
rcCloudIqPollUrl	1.3.6.1.4.1.2272.1.230.1.1.13	8.1.1
rcCloudIqMonitorFreq	1.3.6.1.4.1.2272.1.230.1.1.14	8.1.1
rcCloudIqPollFreq	1.3.6.1.4.1.2272.1.230.1.1.15	8.1.1
rcCloudIqLastOnboardTime	1.3.6.1.4.1.2272.1.230.1.1.16	8.1.1
rcCloudIqLastPollStatus	1.3.6.1.4.1.2272.1.230.1.1.17	8.1.1
rcCloudIqLastPollTime	1.3.6.1.4.1.2272.1.230.1.1.18	8.1.1
rcCloudIqLastMonitorStatus	1.3.6.1.4.1.2272.1.230.1.1.19	8.1.1
rcCloudIqLastMonitorTime	1.3.6.1.4.1.2272.1.230.1.1.20	8.1.1
rcCloudIqLastHealthStatus	1.3.6.1.4.1.2272.1.230.1.1.21	8.1.1
rcCloudIqLastHealthTime	1.3.6.1.4.1.2272.1.230.1.1.22	8.1.1
rcnCloudIqUpTrap	1.3.6.1.4.1.2272.1.21.0.357	8.1.1
rcnCloudIqDownTrap	1.3.6.1.4.1.2272.1.21.0.358	8.1.1
rcIsisLogicalInterfaceMtu	1.3.6.1.4.1.2272.1.63.26.1.17	8.1.50
rcIsisLogicalInterfaceIpsecResponderOnly	1.3.6.1.4.1.2272.1.63.26.21	8.1.50
rcIsisLogicalInterfaceIpsecRemoteNatIPAddr	1.3.6.1.4.1.2272.1.63.26.22	8.1.50
rcPrQosCosQueTunnelStatsTable	1.3.6.1.4.1.2272.1.202.1.1.1.21	8.1.50
rcSysDnsDomainNameOrigin	1.3.6.1.4.1.2272.1.1.128	8.2
rcSysDnsAdvertisedHostName	1.3.6.1.4.1.2272.1.1.129	8.2
rcVlanIsidName	1.3.6.1.4.1.2272.1.3.2.1.80	8.2

Table continues…

Object Name	Object OID	New in VOSS Release
rcIpConfBfdEnable	1.3.6.1.4.1.2272.1.8.1.1.1.25	8.2
rcIpConfBfdTable	1.3.6.1.4.1.2272.1.8.1.12	8.2
rcIpAdEntName	1.3.6.1.4.1.2272.1.8.2.1.13	8.2
rcIpStaticRouteName	1.3.6.1.4.1.2272.1.8.15.2.1.11	8.2
rcIpBfd	1.3.6.1.4.1.2272.1.8.104	8.2
rcIpv6StaticRouteName	1.3.6.1.4.1.2272.1.62.1.1.6.1.10	8.2
rcIsisGlobalMgmtClipIpAddr	1.3.6.1.4.1.2272.1.63.1.26	8.2
rcIsisLogicalInterfaceBfdEnable	1.3.6.1.4.1.2272.1.63.26.1.20	8.2
rcIsisLogicalInterfaceEncryptionKeyLength	1.3.6.1.4.1.2272.1.63.26.18	8.2
rcIsisLogicalInterfaceIpsecTunnelDestAddress	1.3.6.1.4.1.2272.1.63.26.19	8.2
rcBfd	1.3.6.1.4.1.2272.1.81	8.2
rcIsidInterfaceIsidName	1.3.6.1.4.1.2272.1.87.5.1.8	8.2
rcIsidGlobalNameTable	1.3.6.1.4.1.2272.1.87.6	8.2
rcIsisGlobalIpsecTunnelSourceAddress	1.3.6.1.4.1.2272.1.200.1.25	8.2
rcVrfIpVpnIsidName	1.3.6.1.4.1.2272.1.203.1.1.4.1.10	8.2
rcVrfIpv6IpVpnIsidName	1.3.6.1.4.1.2272.1.203.1.1.7.1.8	8.2
rcIsidServiceName	1.3.6.1.4.2272.1.87.2.1.8	8.2

Obsolete MIBs

Table 45: Common

Object Name	Object OID	Obsolete in VOSS Release
rcSysForceTrapSender	1.3.6.1.4.1.2272.1.1.57	8.1.60
rcSysTrapRecvTable	1.3.6.1.4.1.2272.1.1.60	8.1.60
rcSysTrapRecvEntry	1.3.6.1.4.1.2272.1.1.60.1	8.1.60
rcSysTrapRecvAddress	1.3.6.1.4.1.2272.1.1.60.1.1	8.1.60
rcSysTrapRecvVersion	1.3.6.1.4.1.2272.1.1.60.1.2	8.1.60
rcSysTrapRecvCommunity	1.3.6.1.4.1.2272.1.1.60.1.3	8.1.60
rcSysTrapRecvSrcAddress	1.3.6.1.4.1.2272.1.1.60.1.4	8.1.60
rcSysTrapRecvRowStatus	1.3.6.1.4.1.2272.1.1.60.1.5	8.1.60
rcSysTrapSenderTable	1.3.6.1.4.1.2272.1.1.62	8.1.60

Table continues…

Object Name	Object OID	Obsolete in VOSS Release
rcSysTrapSenderEntry	1.3.6.1.4.1.2272.1.1.62.1	8.1.60
rcSysTrapSenderRecvAddress	1.3.6.1.4.1.2272.1.1.62.1.1	8.1.60
rcSysTrapSenderSrcAddress	1.3.6.1.4.1.2272.1.1.62.1.2	8.1.60
rcSysForceIpHdrSender	1.3.6.1.4.1.2272.1.1.68	8.1.60
rcRadiusGlobalSourceIpFlag	1.3.6.1.4.1.2272.1.29.1.16	8.1.60
rcRadiusServHostSourceIpAddr	1.3.6.1.4.1.2272.1.29.5.1.30	8.1.60
rcTacacsServerSourceIpInterfaceEnabled	1.3.6.1.4.1.2272.1.65.2.1.8	8.1.60
rcTacacsServerSourceIpInterfaceType	1.3.6.1.4.1.2272.1.65.2.1.9	8.1.60
rcTacacsServerSourceIpInterface	1.3.6.1.4.1.2272.1.65.2.1.10	8.1.60
rcSyslogGlobalHeader	1.3.6.1.4.1.2272.1.22.1.4	8.1.60
rcnAuthenticationSuccess	1.3.6.1.4.1.2272.1.21.0.268	8.2

Table 46: VSP 4900 Series

Object Name	Object OID	Obsolete in VOSS Release
pethFastPoeEnable	1.3.6.1.2.1.105.1.3.1.1.6	8.1.5
pethPerpetualPoeEnable	1.3.6.1.2.1.105.1.3.1.1.7	8.1.5
pethPsePortFastPoeEnable	1.3.6.1.2.1.105.1.1.1.15	8.2
pethPsePortPerpetualPoeEnable	1.3.6.1.2.1.105.1.1.1.16	8.2