ExtremeSwitching™

Release Notes for VSP Operating System Software

Release 6.0.1
9035596
June 2018

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Extreme Networks, Inc. assumes no liability for any errors. Extreme Networks, Inc. reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Extreme Networks shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Extreme Networks. End User agrees to indemnify and hold harmless Extreme Networks, Extreme Networks' agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Extreme Networks is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Extreme Networks. Extreme Networks is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Extreme Networks does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Extreme Networks provides a limited warranty on Extreme Networks hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Extreme Networks' standard warranty language, as well as information regarding support for this product while under warranty is available to Extreme Networks customers and other parties through the Extreme Networks Support website: http://www.extremenetworks.com/support under the link ""Policies" or such successor site as designated by Extreme Networks. Please note that if You acquired the product(s) from an authorized Extreme Networks Channel Partner outside of the United States and Canada, the warranty is provided to You by said Extreme Networks Channel Partner and not by Extreme Networks.

"Hosted Service" means an Extreme Networks hosted service subscription that You acquire from either Extreme Networks or an authorized Extreme Networks Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Extreme Networks or Extreme Networks Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS EXTREME NETWORKS SOFTWARE, PURCHASED FROM EXTREME NETWORKS, INC., ANY EXTREME NETWORKS AFFILIATE, OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY EXTREME NETWORKS IN WRITING, EXTREME NETWORKS DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN EXTREME NETWORKS, AN EXTREME NETWORKS AFFILIATE OR AN EXTREME NETWORKS CHANNEL PARTNER; EXTREME NETWORKS RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND EXTREME NETWORKS, INC. OR THE APPLICABLE EXTREME NETWORKS AFFILIATE ("EXTREME NETWORKS").

Extreme Networks grants You a license within the scope of the license types described below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Extreme Networks or an Extreme Networks Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Extreme Networks in writing. Extreme Networks may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Extreme Networks through electronic means established by Extreme Networks specifically for this purpose.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Extreme Networks can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Extreme Networks Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Extreme Networks’ website at:http://www.extremenetworks.com/support/policies/software-licensing or such successor site as designated by Extreme Networks. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO EXTREME NETWORKS CHANNEL PARTNER’S HOSTING OF EXTREME NETWORKS PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN EXTREME NETWORKS CHANNEL PARTNER’S HOSTING OF EXTREME NETWORKS PRODUCTS MUST BE AUTHORIZED IN WRITING BY EXTREME NETWORKS AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE EXTREME NETWORKS CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE EXTREME NETWORKS CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Extreme Networks product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Security Vulnerabilities

Information about Extreme Networks’ security support policies can be found in the Global Technical Assistance Center Knowledgebase at https://gtacknowledge.extremenetworks.com/.

Downloading Documentation

For the most current versions of Documentation, see the Extreme Networks Support website: http://documentation.extremenetworks.com, or such successor site as designated by Extreme Networks.

Contact Extreme Networks Support

See the Extreme Networks Support website:http://www.extremenetworks.com/support for product or Hosted Service notices and articles, or to report a problem with your Extreme Networks product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Extreme Networks Support website:http://www.extremenetworks.com/support/contact/ (or such successor site as designated by Extreme Networks), scroll to the bottom of the page, and select Contact Extreme Networks Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Extreme Networks are the registered or unregistered Marks of Extreme Networks, Inc., its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Extreme Networks or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Extreme Networks or the applicable third party.

Extreme Networks is a registered trademark of Extreme Networks, Inc.

All non-Extreme Networks trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

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

Contents

Chapter 1: Preface

Disclaimer

On July 15, 2017, Extreme Networks acquired the Networking Business Unit from Avaya. In some cases the Avaya name is specific to command syntax, in those cases Avaya may continue to appear in the documentation and the operational software. Where applicable the documentation will continue to use the name of Avaya products that did not transition to Extreme Networks with which the networking products have unique operational capabilities

Purpose

This document provides information on features in VSP Operating System Software (VOSS). VOSS runs on the following product families:

- Extreme Networks Virtual Services Platform 4000 Series
- Extreme Networks Virtual Services Platform 7200 Series
- Extreme Networks Virtual Services Platform 8000 Series (includes VSP 8200 and VSP 8400 Series)
- Extreme Networks Virtual Services Platform 8600

This document describes important information about this release for the VOSS products.

These Release Notes include supported hardware and software, scaling capabilities, and a list of known issues (including workarounds, where appropriate). This document also describes known limitations and restrictions.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at www.extremenetworks.com/education/.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

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

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at internalinfodev@extremenetworks.com

Getting Help

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

- GTAC (Global Technical Assistance Center) for Immediate Support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal – Manage cases, downloads, service contracts, product licensing, and training and certifications.

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

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

Extreme Networks Documentation

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

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for previous versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing.

Subscribing to Service Notifications

Subscribe to receive an email notification for product and software release announcements, Vulnerability Notices, and Service Notifications.

About this task

You can modify your product selections at any time.

Procedure

1. In an Internet browser, go to http://www.extremenetworks.com/support/service-notification-form/ .
2. Type your first and last name.
3. Type the name of your company.
4. Type your email address.
5. Type your job title.
6. Select the industry in which your company operates.
7. Confirm your geographic information is correct.
8. Select the products for which you would like to receive notifications.
9. Click **Submit**.

Chapter 2: New in this release

The following sections detail what is new in *Release Notes*.

Release 6.0.1 features

See the following section for information about feature changes.

New hardware

VOSS 6.0.1 introduces the following new hardware:

- New 40 Gigabit Ethernet QSFP+ transceiver:
  - 40GBASE-SR4 (extended short reach) 4x10GBASE-SR QSFP+, AA1404006-E6

Distributed Virtual Routing

Stretching IP subnets across multiple locations, racks in a data center and floors or buildings in a wireless deployment, enables hosts (virtual machines or wireless users) to move around freely without changing their IP addresses. However, when IP subnets are stretched, inefficient routing (traffic tromboning) can occur because the default gateway router might not be local to the roaming hosts.

Distributed Virtual Routing (DvR) addresses this problem by distributing the routing instance to all switches that have an IP interface in the IP subnet or VLAN. Virtual machines use their first hop Top of the Rack (TOR) switches to be their default gateways. In wireless deployments users can roam between buildings and each building provides default gateway routing capabilities for the users, thus distributing the load and optimizing traffic patterns.

By solving the problem of inefficient routing caused by the Trombone effect, DvR effectively reduces latency in real-time applications such as voice and video.

Note:

Release 6.0.1 provides full support for Distributed Virtual Routing (DvR) for all platforms except for VSP 4000, which supports DvR as a demo feature only.

DvR requires a Premier license.

For more information, see *Configuring IPv4 Routing*.

Release 6.0 features

See the following section for information about feature changes.

New hardware

VOSS 6.0 introduces the following new hardware:

- New 10 Gigabit Ethernet SFP Transceiver:
  - 10GBASE-T SFP, AA1403043-E6

Bridge Protocol Data Unit (BPDU) Guard

The Spanning Tree Protocol detects and eliminates logical loops in a bridged or switched network. Any bridge that participates in the spanning tree exchanges information with other bridges using configuration messages known as Bridge Protocol Data Units (BPDU). Based on the BPDU information exchange, the bridge with the lowest bridge ID becomes the root.To ensure the correct operation of Spanning Tree in the network, BPDU Guard protects the stability of the Root Bridge by dropping stray, unexpected, or unwanted BPDU packets entering a port, and immediately shutting down those ports for a specified time period. BPDU Guard is normally enabled on access ports connecting to end user devices such as servers that are not expected to operate Spanning Tree.

For more information, see *Configuring VLANs, Spanning Tree, and NLB*.

EDM support for viewing licenses

You can now use EDM to view information about the license file on the switch.

For more information, see *Administering*.

Entity MIB - Physical Table

The Entity MIB - Physical Table assists in the discovery of functional components on the switch. The Entity MIB - Physical Table supports a physical interface table that includes information about the chassis, power supply, fan, I/O cards, console, and management port.

For more information, see *Administering*.

Fabric Attach Zero Touch Client Attachment

Fabric Attach Zero Touch Client Attachment provides the ability for an FA client to automatically attach to an existing Shortest Path Bridging Network and provide for automatic configuration of the service identifier (I-SID) and virtual LAN based on FA client element type. FA clients must signal the desire to join an SPB network through the use of specific LLDP TLVs.

For more information, see *Configuring Fabric Connect*.

Fabric RSPAN (Mirror to I-SID)

With Fabric RSPAN (Mirror to I-SID) feature, mirrored traffic captured from any switch in the network is sent to a remote switch over an SPB cloud for traffic analysis. With this feature, you can monitor traffic on ports from different switches connected in the network using just one network analyzer connected to a remote switch which acts as a collector. The source device where the traffic is mirrored to an I-SID is known as Mirroring BEB (Backbone Edge Bridge), and the remote device where the traffic analyzer is connected for mirrored traffic analysis is known as Monitoring BEB.

Remote mirroring of traffic is not supported on NNI ports, Fabric Extend Layer 2 core ports, and Open Networking Adapter (ONA) devices and ports.

For more information, see *Troubleshooting*.

Forgiving mode for CWDM and DWDM SFP+ transceivers

The switch now operates in forgiving mode for coarse wave division multiplexing (CWDM) and dense wave division multiplexing (DWDM) SFP+ transceivers. For all other SFP+ transceivers, the switch continues to operate in strict mode.

For more information, see *Installing Transceivers and Optical Components*.

Increased VRF and L3 VSN scaling

You can now use a boot config flag to increase the number of Virtual Routing and Forwarding (VRF) instances on the switch from the previous maximum of 24. This enhancement also impacts the number of Layer 3 Virtual Services Networks (VSN). The maximum number of supported VRFs and Layer 3 VSNs differs depending on the hardware platform.

❗ **Important:**

> If you use the boot config flag to increase the number of VRFs and Layer 3 VSNs, and the switch operates in SPBM mode, the switch reduces the number of configurable VLANs.

A Premier or Premier + MACsec license is required to use more than 24 VRFs.

For more information, see *Configuring IPv4 Routing*.

Industry Standard Discovery Protocol (ISDP) (CDP compatible)

Industry Standard Discovery Protocol (ISDP) is a CDP compatible discovery protocol used to detect directly connected networking equipment.

For more information, see *Administering*.

IPsec for the Out-of-band management port

This release adds IPsec support for IPv6 traffic on the out-of-band management interface.

For more information, see *Configuring Security*.

IEEE 802.3x Pause frame transmit

This release introduces support for flow control mode and the ability for an interface to send pause frames. When congestion occurs on an egress port, the system can send pause frames to the offending devices to stop the packet flow. The system uses flow control if the rate at which one or more ports receives packets is greater than the rate at which the switch transmits packets.

For more information, see the following documents:

- *Administering*
- *Monitoring Performance*

Link Layer Discovery Protocol (LLDP)

This release introduces support for Link Layer Discovery Protocol (LLDP) which has been standardized by the IEEE as part of 802.1ab. LLDP enables you to advertise your identity and capabilities and obtain the same information from a physically adjacent Layer 2 peer to detect and correct network and configuration errors.

For more information, see *Administering*.

MACsec enhancements

MACsec updates in this release enable enhanced security where multiple Secure Association (SA) Keys are internally derived from the configured Connectivity Association Key (CAK), to secure communication on the link. These SA Keys are periodically refreshed to ensure that the same key is not used for an extended period of time. From a provisioning perspective, the administrator still configures a single shared CAK on the two ends of the MACsec enabled link. This CAK is now used to internally derive multiple SA Keys. In order to differentiate the transmit and receive SA keys used between two ends of a MACsec enabled link, one additional parameter has been added (`key-parity <even|odd>`). MACsec links should always be provisioned as odd/even pair.

After the upgrade, previously configured MACsec links will continue to be operational with earlier MACsec implementations where fewer SAs were used to secure the link. In order to utilize the enhanced security, it is strongly recommended to add the `key-parity` configuration, which will enable multiple SA keys to be used to secure the link. This enhancement will also require CAK to be a minimum of 20 characters to ensure derivation of stronger keys.

Note:

> With this release, `key-parity` is an optional parameter. Future releases will make this a mandatory parameter. As such, to avoid configuration breaks during upgrade to future releases, it is strongly recommended that once you upgrade to VOSS 6.0, you should update your existing MACsec configuration to include the `key-parity` keyword and provision the MACsec links as odd/even pairs.

MACsec requires a Premier license.

For more information, see *Configuring Security*.

Network Load Balancing (NLB) Multicast operation

When you enable NLB multicast mode on a VLAN, the routed traffic destined to the NLB cluster is flooded by default on all ports of the VLAN. All VLANs support multiple cluster IPs by default.

Multicast MAC flooding and static multicast ARP entries are not supported for NLB Unicast or NLB Multicast in this release.

For more information, see *Configuring VLANs, Spanning Tree, and NLB*.

nni-mstp boot config flag

The default value for the nni-mstp flag is false. In previous releases, MSTP was enabled for the CIST and all MSTIs other than MSTI-62. In the current release, the default behavior of the MSTP on SPBM NNI ports is that CIST is disabled automatically on the NNI and the NNI ports cannot be members of any VLANs other than B-VLANs. You can override this by setting the nni-mstp flag to true, which disables MSTP on MSTI-62, and allows any VLAN to be configured on NNI ports.

On SPBM NNI links, MSTP is disabled and no VLAN, except SPBM B-VLANs can be added. When nni-mstp flag is set to true, it only disables MSTI 62 and additional VLANs on other MSTIs can be added to NNI links.

Important:

> **Before you upgrade**
>
> If you upgrade to a new release that introduces support for the **boot config flags nni-mstp command**, and your previous configuration included coexistence of MSTP and SPB-based

services on the NNI ports in the configuration file or your current release supports the nni-mstp boot configuration and the flag is set to false, take note of the following:

During startup, your configuration file will load successfully with only one change, in that the nni-mstp flag is set to true. Your system will operate the same as before upgrading. Save the configuration file. If you do not save your configuration, you continue to see the following message on reboot:

```
Warning Detected brouter and/or vlans other than BVLANs on NNI ports.
Setting the boot config flag nni-mstp to true. Saving configuration
avoids repetition of this warning on reboot.
```

For more information, see *Administering*.

Simple Mail Transfer Protocol (SMTP) for log notification

The switch supports the SMTP feature to send email notification of failed components or other critical log-event conditions. The switch can also send periodic health status notifications.

For more information, see the following documents:

- *Troubleshooting*
- *Monitoring Performance*
- *Administering*

sFlow

sFlow monitors the traffic on routers and switches in a network, and captures traffic statistics about those devices. Because sFlow performs random samples and periodic counter samples, it is scalable for network-wide monitoring, which includes high speed networks.

For more information, see *Monitoring Performance*.

SPB-PIM Gateway

SPB-PIM Gateway (SPB-PIM GW) provides multicast inter-domain communication between an SPB network and a Protocol Independent Multicast (PIM) network. SPB-PIM GW accomplishes this inter-domain communication across a special gateway VLAN. The gateway VLAN communicates with the PIM network through the PIM protocol messaging and translates the PIM network requirements into SPB language and vice versa.

For more information, see *Configuring SPB-PIM Gateway*.

SSH client disable

This release adds the ability to disable the SSH client in the software.

For more information, see *Administering*.

VXLAN Gateway

VXLAN Gateway is a hardware-based virtual tunnel end point (VTEP) that terminates virtual extensible LAN (VXLAN) tunnels. The VXLAN tunnels “stretch” emulated Layer 2 segments over an IP network. Each VTEP has at least one segment ID called a VXLAN Network Identifier (VNID). This VNID mechanism allows up to *16 million* VXLAN segments to coexist within the same administrative domain. Each VTEP can support multiple VNIDs.

The VXLAN Gateway feature provides a solution that allows VXLANs to seamlessly communicate with traditional VLANs, other VXLANs, or Fabric Connect I-SIDs. For more information about VXLAN, see the Internet Engineering Task Force (IETF) standard RFC 7348.

VXLAN Gateway requires a Premier license.

For more information, see *Configuring VLANs, Spanning Tree, and NLB*.

VOSS feature differences

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

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

Feature	VSP 4000 Series	VSP 7200 Series	VSP 8000 Series
Channelization of 40 Gbps ports	Not applicable	Supported	Supported
CFM CMAC for the C-VLAN	Supported	Not supported	Not supported
DvR Controller	Not supported	Supported	Supported
DvR Leaf	Demo only	Supported	Supported
Endura scripts	Supported	Not supported	Not supported
Fabric RSPAN	Flow-based Mirroring into single ISID only	Supported	Supported
FDB protected by port	Supported	Not supported	Not supported
Ingress Dual Rate Port Policers	Supported	Not supported	Not supported
MAC FDB Protect by port	Supported	Not supported	Not supported
MAC security limit-learning	Supported	Not supported	Not supported
Multicast Route Statistics for IPv4 and IPv6	Not supported	Supported	Supported
NLB Unicast and Multicast	Not supported	Supported	Supported
SPM-PIM GW Controller	Supported	Supported	Supported
SPM-PIM GW Interface	Supported	Supported	Supported

Table continues…

Feature	VSP 4000 Series	VSP 7200 Series	VSP 8000 Series
PoE/PoE+ Allocation Using LLDP	Supported on VSP 4850GTS-PWR+ and VSP 4450GTX-HT-PWR+	Not supported	Not supported
Port licensing	Not supported	Applicable to Port licensed VSP 7254XSQ fiber switch and VSP 7254XTQ copper switch	Not supported
QoS	Supported	Supported with exceptions: • Classification does not have routed packet classification • No ingress policer-Uses ingress port rate limiting instead	Supported with exceptions: • Classification does not have routed packet classification • No ingress policer-Uses ingress port rate limiting instead
sFLOW	Reduced sampling rate	Supported	Supported
Software licensing (Premier)	Supports licenses generated from the Avaya Data Licensing Portal and the Product Licensing & Delivery System (PLDS)	Supports licenses generated from the Product Licensing & Delivery System (PLDS) only	Supports licenses generated from the Product Licensing & Delivery System (PLDS) only
Use of Open Networking Adapt er for Fabric Extend	Required	Not required	Not required
VXLAN Gateway	Not supported	Supported	Supported

Documentation changes

The following changes have been made to the Documentation suite in this release.

Relocation of image upgrade information

The information on image upgrade has been moved from *Release Notes* to *Administering*.

For more information, see *Administering*.

Resources

Information about related resources is moved to the last chapter in this document.

Support changes

This release makes the following support changes to pre-existing features.

ECMP support for VXLAN Gateway and Fabric Extend

VXLAN Gateway requires ECMP support to communicate with remote VTEPs. The software extended this ECMP support to Fabric Extend Layer 3 core tunnels. Therefore, if your switch supports VXLAN Gateway, it also supports ECMP for both VXLAN Gateway and Fabric Extend.

Fabric Extend IP over ELAN/VPLS enhancement

This release removes the single next hop / ARP restriction on VSP 7200 and VSP 8000 series switches. 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.

SPB Ethertype – change in behavior on NNI

SPB switches now follow the configured Ethertype on egress from NNI interfaces. On ingress the switches will honor Ethertype of either 0x8100 and 0x88a8.

Chapter 3: Important notices

This section describes the supported hardware and software scaling capabilities, and provides important information for this release. Unless specifically stated otherwise, the notices in this section apply to all VOSS platforms.

Hardware compatibility

This section lists the hardware compatibility for all VOSS platforms.

Hardware compatibility for VSP 4000 Series

This section lists the Virtual Services Platform 4000 Series hardware and indicates the software release support.

Note:

4.1 is the first VOSS release. Release numbers earlier than 4.1 are releases specific to VSP 4000.

Part numbers that end in GS are the TAA-compliant version of the hardware.

VSP 4000 hardware

Part number	Model number	Initial release	Supported release					
			4.2.1	5.0	5.1	5.1.1	6.0	6.0.1
EC4400004-E6	VSP 4450GSX-DC	4.0.50	—	Y	Y	Y	Y	Y
EC4400A03-E6	VSP 4450GTX-HT-PWR+ (no power cord)	4.0.40	Y	Y	Y	Y	Y	Y
EC4400E03-E6	VSP 4450GTX-HT-PWR+ (NA power cord)	4.0.40	Y	Y	Y	Y	Y	Y
EC4400x05-E6 Note: Replace the “x” with a country specific power cord	VSP 4450GSX-PWR+	4.0	Y	Y	Y	Y	Y	Y

Table continues…

Part number	Model number	Initial release	Supported release					
			4.2.1	5.0	5.1	5.1.1	6.0	6.0.1
code. See the footnote for details.								
EC4400A05-E6GS	VSP 4450GSX-PWR+ TAA Compliant (no power cord)	4.0.50	Y	Y	Y	Y	Y	Y
EC4400E05-E6GS	VSP 4450GSX-PWR+ TAA Compliant (NA power cord)	4.0.50	Y	Y	Y	Y	Y	Y
EC4800078-E6	VSP 4850GTS DC	3.0	Y	Y	Y	Y	Y	Y
EC4800x78-E6 EC4800x78-E6GS Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 4850GTS	3.0	Y	Y	Y	Y	Y	Y
EC4800x88-E6 EC4800x88-E6GS Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 4850GTS-PWR+	3.0	Y	Y	Y	Y	Y	Y

Note: The character (x) in the order number indicates the power cord code. Replace the “x” with the proper letter to indicate the desired product nationalization. See the following for details:

“A”: No power cord included.

“B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden.

“C”: Includes power cord commonly used in the United Kingdom and Ireland.

“D”: Includes power cord commonly used in Japan.

“E”: Includes North American power cord.

“F”: Includes Australian power cord.

Compatible transceivers

Important:

Use Extreme-branded SFP, and SFP+ transceivers as they have been through extensive qualification and testing. Extreme will not be responsible for issues related to non-Extreme branded transceivers.

- The VSP 4000 Series operates in forgiving mode for SFP transceivers, which means that the switch will bring up the port operationally when using non-Extreme SFP transceivers. Extreme does not provide support for operational issues related to these SFPs, but they will operate and the port link will come up. The switch logs the device as an unsupported or unknown device.
- The VSP 4000 Series operates in forgiving mode for coarse wave digital multiplexing (CWDM) and dense wave digital multiplexing (DWDM) SFP+ transceivers, and will bring the port up operationally when using non-Extreme SFP+ transceivers. For all other SFP+ transceivers, the switch operates in strict mode, which means that the switch will not bring the port up operationally when using non-Extreme SFP+ transceivers.
- The VSP 4000 Series operates in forgiving mode for SFP+ direct attached cables, which means that the switch will bring up the port operationally when using Non-Extreme direct attached cables. Extreme does not provide support for operational issues related to these DACs, but they will operate and the port link will come up.

For more information about compatible transceivers, see *Installing Transceivers and Optical Components on VSP Operating System Software*, NN47227-301.

Important operational note for VSP 4000 switches

This section provides information to take into consideration to prevent system operation failure.

Operational consideration for USB Flash Drive on factory supplied and converted VSP 4000 switches
Warning: The USB FLASH drive on all models of VSP 4850 (factory built and converted from ERS 4850) must be treated as a permanent non-removable part of the switch and must NEVER be removed from the switch to ensure proper operation. Additionally, the USB cover must be installed to ensure additional protection against removal. The USB FLASH drive on the VSP 4850 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.

Hardware compatibility for VSP 7200 Series

This section lists the VSP 7200 Series hardware and indicates the software release support.

VSP 7200 hardware

Part number	Model number	Initial release	Supported release					
			4.2.1	5.0	5.1	5.1.1	6.0	6.0.1
EC720001F-E6	VSP 7254XSQ DC (Front to back airflow)	4.2.1	Y	Y	Y	Y	Y	Y
EC7200x1B-E6 EC7200x1F-E6 B represents back to front airflow. F represents front to back airflow. Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 7254XSQ	4.2.1	Y	Y	Y	Y	Y	Y
EC720002F-E6	VSP 7254XTQ DC (Front to back airflow)	4.2.1	Y	Y	Y	Y	Y	Y
EC7200x2B-E6 EC7200x2F-E6 B represents back to front airflow. F represents front to back airflow. Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 7254XTQ	4.2.1	Y	Y	Y	Y	Y	Y
EC7200x3B-E6 EC7200x3F-E6 B represents back to front airflow. F represents front to back airflow. Note: Replace the “x” with a country specific power cord code. See	VSP 7254XSQ Port Licensed	5.1	N/A	N/A	Y	Y	Y	Y

Table continues…

Part number	Model number	Initial release	Supported release					
			4.2.1	5.0	5.1	5.1.1	6.0	6.0.1
the footnote for details.								
EC7200x4B-E6 EC7200x4F-E6 B represents back to front airflow. F represents front to back airflow. Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 7254XTQ Port Licensed	5.1	N/A	N/A	Y	Y	Y	Y
***Note**: The character (x) in the order number indicates the power cord code. Replace the “x” with the proper letter to indicate desired product nationalization. See the following for details: “A”: No power cord included. “B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden. “C”: Includes power cord commonly used in the United Kingdom and Ireland. “D”: Includes power cord commonly used in Japan. “E”: Includes North American power cord. “F”: Includes Australian power cord.								

Compatible transceivers

Important:

Use Extreme-branded SFP, SFP+, and QSFP+ transceivers as they have been through extensive qualification and testing. Extreme will not be responsible for issues related to non-Extreme branded transceivers.

- The VSP 7200 Series operates in forgiving mode for SFP transceivers, which means that the switch will bring up the port operationally when using non-Extreme SFP transceivers. Extreme does not provide support for operational issues related to these SFPs, but they will operate and the port link will come up. The switch logs the device as an unsupported or unknown device.
- The VSP 7200 Series operates in strict mode for some SFP+ and QSFP+ transceivers, which means that the switch will not bring the port up operationally when using non-Extreme SFP+ or QSFP+ transceivers. For coarse wave digital multiplexing (CWDM) and dense wave digital multiplexing (DWDM) SFP+ transceivers, the switch operates in forgiving mode and will bring up the port operationally when using non-Extreme SFP+ transceivers of these types.

- The VSP 7200 Series operates in forgiving mode for SFP+ and QSFP+ direct attached cables, which means that the switch will bring up the port operationally when using non-Extreme direct attached cables. Extreme does not provide support for operational issues related to these DACs, but they will operate and the port link will come up.

For more information about compatible transceivers, see *Installing Transceivers and Optical Components on VSP Operating System Software*, NN47227-301.

VSP 7200 operational notes

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

    The AA1403165 10GBASE-ZR CWDM DDI SFP+ transceiver can be substituted for AA1403016-E6 10GBASE-ZR/ZW SFP+.
- Software partitions the switch into two logical slots: Slot 1 and Slot 2.
  - Slot 1: 10 Gbps ports: 1 - 48
  - Slot 2: 40 Gbps ports: 1 - 6
- Channelization is supported on the 40 Gbps QSFP+ ports.
- MACsec support:
  - MACsec is only supported on the VSP 7254XTQ 10 Gbps ports.
  - MACsec is not supported on VSP 7254XSQ 10 Gbps ports.
  - MACsec is not supported on VSP 7254XTQ and VSP 7254XSQ 40 Gbps ports whether channelization is enabled or not.
- Port licensing support:

  On the port licensed VSP 7254XSQ fiber switch:
  - 24 ports (Slot 1, ports 25 to 48) out of the 48 1/10 GbE SFP/SFP+ ports require a Port License to be unlocked.
  - two ports (Slot 2, ports 5 and 6) out of the six 40 GbE QSFP+ ports require a Port License to be unlocked.

  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.
- Extreme recommends enabling 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.

For more information, see *Installing Transceivers and Optical Components on VSP Operating System Software*, NN47227-301.

Hardware compatibility for VSP 8000 Series

This section lists the VSP 8000 Series hardware and indicates the software release support.

Note:

4.1 is the first VOSS release. Release numbers earlier than 4.1 are releases specific to VSP 8000.

Part numbers that end in GS are the TAA-compliant version of the hardware.

VSP 8000 hardware

Part number	Model number	Initial release	Supported release					
			4.2.1	**5.0**	**5.1**	**5.1.1**	**6.0**	**6.0.1**
EC8200x01-E6 EC8200x01-E6GS Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 8284XSQ	4.0	Y	Y	Y	Y	Y	Y
EC8200001-E6	VSP 8284XSQ-DC	4.0.50	Y	Y	Y	Y	Y	Y
EC8400001-E6	VSP 8404-DC	4.2.1	Y	Y	Y	Y	Y	Y
EC8400x01-E6	VSP 8404	4.2	Y	Y	Y	Y	Y	Y

Table continues…

Part number	Model number	Initial release	Supported release					
			4.2.1	**5.0**	**5.1**	**5.1.1**	**6.0**	**6.0.1**
EC8200x01-E6GS Note: Replace the “x” with a country specific power cord code. See the footnote for details.								
Ethernet Switch Modules (ESM) — VSP 8400 only **Important:** Ensure the switch runs, at a minimum, the noted initial software release before you install an ESM.								
EC8404001-E6 EC8404001-E6GS	8424XS	4.2	Y	Y	Y	Y	Y	Y
EC8404002-E6 EC8404002-E6GS	8424XT	4.2	Y	Y	Y	Y	Y	Y
EC8404003-E6 EC8404003-E6GS	8408QQ	4.2	Y	Y	Y	Y	Y	Y
EC8404005-E6 EC8404005-E6GS	8418XSQ	4.2	Y	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
*****Note**: The character (x) in the order number indicates the power cord code. Replace the “x” with the proper letter to indicate desired product nationalization. See the following for details: “A”: No power cord included. “B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden. “C”: Includes power cord commonly used in the United Kingdom and Ireland. “D”: Includes power cord commonly used in Japan. “E”: Includes North American power cord. “F”: Includes Australian power cord.								

Compatible transceivers

Important:

Use Extreme-branded SFP, SFP+, and QSFP+ transceivers as they have been through extensive qualification and testing. Extreme will not be responsible for issues related to non-Extreme branded transceivers.

- The VSP 8000 Series operates in forgiving mode for SFP transceivers, which means that the switch will bring up the port operationally when using non-Extreme SFP transceivers. Extreme does not provide support for operational issues related to these SFPs, but they will operate and the port link will come up. The switch logs the device as an unsupported or unknown device.
- The VSP 8000 Series operates in strict mode for some SFP+ and QSFP+ transceivers, which means that the switch will not bring the port up operationally when using non-Extreme SFP+ or QSFP+ transceivers. For coarse wave digital multiplexing (CWDM) and dense wave digital multiplexing (DWDM) SFP+ transceivers, the switch operates in forgiving mode and will bring up the port operationally when using non-Extreme SFP+ transceivers of these types.
- The VSP 8000 Series operates in forgiving mode for SFP+ and QSFP+ direct attached cables, which means that the switch will bring up the port operationally when using non-Extreme direct attached cables. Extreme does not provide support for operational issues related to these DACs, but they will operate and the port link will come up.

For more information about compatible transceivers, see *Installing Transceivers and Optical Components on VSP Operating System Software*, NN47227-301.

Power supply compatibility

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

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

- *Installing Virtual Services Platform 4850GTS Series*, NN46251-300
- *Installing Virtual Services Platform 4450GTX-HT-PWR+ Switch*, NN46251–304
- *Installing Virtual Services Platform 4450GSX-PWR+ Switch*, NN46251-307
- *Installing the Virtual Services Platform 8000 Series*, NN47227-300
- *Installing the Virtual Services Platform 7200 Series*, NN47228-302

VSP 4000 Series power supplies

Platform	300 W AC	300 W DC	1,000 W AC	1,000 W AC-HT
	AL1905x08-E5	AL1905005-E5	AL1905x21-E6	EC4005x03-E6HT
VSP 4850GTS-DC	—	Y	—	—

Table continues…

Platform	300 W AC AL1905x08-E5	300 W DC AL1905005-E5	1,000 W AC AL1905x21-E6	1,000 W AC-HT EC4005x03-E6HT
VSP 4850GTS-PWR+	—	—	Y	Y
VSP 4850GTS	Y	—	—	—
VSP 4450GTX-HT-PWR+	—	—	—	Y
VSP 4450GSX-DC	—	Y	—	—
VSP 4450GSX-PWR+	—	—	Y	Y

VSP 7200 Series and VSP 8000 Series power supplies

Platform	460 W AC front-to-back EC7205x1F-E6	460 W AC back-to-front EC7205x1B-E6	800 W AC front-to-back EC8005x01-E6	800 W AC front-to-back EC7205x0F-E6	800 W AC back-to-front EC7205x0B-E6	800 W DC front-to-back EC8005001-E6
VSP 8284XSQ	—	—	Y	—	—	—
VSP 8284XSQ-DC	—	—	—	—	—	Y
VSP 8404	—	—	Y	—	—	—
VSP 8404-DC	—	—	—	—	—	Y
VSP 7254XSQ front-to-back	Y	—	—	—	—	—
VSP 7254XSQ back-to-front	—	Y	—	—	—	—
VSP 7254XTQ front-to-back	—	—	—	Y	—	—
VSP 7254XTQ back-to-front	—	—	—	—	Y	—
VSP 7254XSQ-DC	—	—	—	—	—	Y
VSP 7254XTQ-DC	—	—	—	—	—	Y

Note: The character (x) in the order number indicates the power cord code. Replace the “x” with the proper letter to indicate desired product nationalization. See the following for details:

“A”: No power cord included.

“B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden.

“C”: Includes power cord commonly used in the United Kingdom and Ireland.

“D”: Includes power cord commonly used in Japan.

“E”: Includes North American power cord.

“F”: Includes Australian power cord.

Software scaling capabilities

This section lists software scaling capabilities of the following products:

- Virtual Services Platform 4000 Series
- Virtual Services Platform 7200 Series
- Virtual Services Platform 8000 Series

Table 1: Software scaling capabilities

	Maximum number supported		
	VSP 4000 Series	**VSP 7200 Series**	**VSP 8000 Series**
Layer 2			
Directed Broadcast interfaces	n/a	200*	200*
Note: * The number of Directed Broadcast interfaces must be equal to, or less than, 200. However, if you configure VLANs with both **NLB** and **Directed Broadcast**, you can only scale up to 100 VLANs.			
MAC table size (without SPBM)	32,000	224,000	224,000
MAC table size (with SPBM)	16,000	112,000	112,000
Port based VLANs	4,059	4,059	4,059
Private VLANs	1,000	4,059	4,059
Protocol based VLANs (IPv6 only)	1	1	1
RSTP instances	1	1	1
MSTP instances	12	12	12
LACP aggregators	24	54 (up to 72 with channelization)	84 (up to 96 with channelization)

Table continues…

	Maximum number supported		
	VSP 4000 Series	**VSP 7200 Series**	**VSP 8000 Series**
Ports per LACP aggregator	8 active	8 active	8-active
MLT groups	50	54 (up to 72 with channelization)	84 (up to 96 with channelization)
Ports per MLT group	8	8	8
SLPP VLANs	128	128	128
VLACP interfaces	50	54 (up to 72 with channelization)	84 (up to 96 with channelization)
Microsoft NLB cluster IP interfaces	n/a	200*	200*

Note:

* The number of NLB cluster IP interfaces multiplied by the number of configured clusters must be less than or equal to 200. The number of NLB cluster IP interfaces is the key, not the number of VLANs. You can configure 1 VLAN with up to 200 NLB cluster IP interfaces or configure up to 200 VLANs with 1 NLB cluster IP interface per VLAN.

For example: `1 NLB cluster IP interface x 200 clusters = 200` or `2 NLB cluster IP interfaces 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			
IP interfaces (IPv4 or IPv6 or IPv4+IPv6)	256	506*	506*
VRRP interfaces (IPv4 or IPv6)	64	252*	252*
Routed Split Multi-Link Trunking (RSMLT) interfaces (IPv4 or IPv6 or IPv4+IPv6)	252	252*	252*

Note:

* The maximum number of IP interfaces is based on the following formulas:

- If you *disable* the VRF scaling boot configuration flag:

  ```
  = 506 - (# of VRRP IPv4 interfaces) - (# of VRRP IPv6 interfaces) - (# of
  RSMLT interfaces) -2 (if IP Shortcuts is enabled) - 3x(# of VRFs)
  ```

- If you *enable* the VRF scaling boot configuration flag:

  ```
  = 506 - (# of VRRP IPv4 interfaces) - (# of VRRP IPv6 interfaces) - (# of
  RSMLT interfaces) -2 (if IP Shortcuts is enabled) - 3
  ```

Table continues…

	Maximum number supported		
	VSP 4000 Series	**VSP 7200 Series**	**VSP 8000 Series**
VRRP interfaces with fast timers (200ms) - IPv4/ IPv6	24	24	24
DvR Virtual IP interfaces	n/a	501 with vIST 502 without vIST	501 with vIST 502 without vIST
ECMP groups/paths per group	500/4	1,000/8	1,000/8
OSPF v2/v3 interfaces	100	500	500
OSPF v2/v3 neighbors (adjacencies)	100	500	500
OSPF areas	12 for each VRF 64 for the switch	12 for each VRF 80 for the switch	12 for each VRF 80 for the switch
IPv4 ARP table	6,000	32,000	32,000
IPv4 CLIP interfaces	64	64	64
IPv4 RIP interfaces	24	200	200
IPv4 BGP peers	12	12	12
IPv4 VRF instances	128 including mgmt VRF and GRT	256 including mgmt VRF and GRT	256 including mgmt VRF and GRT
IPv4 static ARP entries	200 for each VRF 1,000 for the switch	2,000 for each VRF 10,000 for the switch	2,000 for each VRF 10,000 for the switch
IPv4 static routes	1,000 for each VRF 1,000 for the switch	1,000 for each VRF 5,000 for the switch	1,000 for each VRF 5,000 for the switch
IPv4 route policies	500 for each VRF 5,000 for the switch	500 for each VRF 5,000 for the switch	500 for each VRF 5,000 for the switch
IPv4 UDP forwarding entries	128	512	512
IPv4 DHCP Relay forwarding entries	128	1,024	1,024
IPv6 DHCP Snoop entries in Source Binding Table	1,024	1,024	1,024
IPv6 Neighbor table	4,000	8,000	8,000
IPv6 static entries in Source Binding Table	256	256	256
IPv6 static neighbor records	128	256	256
IPv6 CLIP interfaces	64	64	64

Table continues…

	Maximum number supported		
	VSP 4000 Series	**VSP 7200 Series**	**VSP 8000 Series**
IPv6 static routes	1,000	1,000	1,000
IPv6 6in4 configured tunnels	254	506	506
IPv6 DHCP Relay forwarding	128	512	512
IPv6 RIPng interfaces	24	48	48
Layer 3 route table entries			
IPv4 RIP routes	See Table 2: IPv4 and IPv6 route scaling on page 33.		
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			
IP Multicast			
Combination of VLANs + number of IPv4 senders + IPv6 senders (non-SPBM mode)	4,059	8,192	8,192
Combination of Layer 2 VSNs + number of IPv4 senders + number of IPv6 senders (SPBM mode)	4,059	8,192	8,192
IGMP/MLD interfaces (IPv4/IPv6)	4,059	4,059	4,059
PIM interfaces (IPv4/IPv6)	128 Active	128 Active	128 Active
PIM Neighbors (IPv4/ IPv6) (GRT Only)	128	128	128
PIM-SSM static channels (IPv4/IPv6)	512	4,000	4,000
Multicast receivers/IGMP joins (IPv4/IPv6) (per switch)	1,000	6,000	6,000

Table continues…

	Maximum number supported		
	VSP 4000 Series	**VSP 7200 Series**	**VSP 8000 Series**
Total multicast routes (S,G,V) (IPv4/IPv6) (per switch)	1,000	6,000	6,000
Total multicast routes (S,G,V) (IPv4) on a PIM-Gateway configured switch	1,000	3,000	3,000
Static multicast routes (S,G,V) (IPv4/IPv6)	512	4,000	4,000
Multicast enabled Layer 2 VSN (IPv4)	1,000	2,000	2,000
Multicast enabled Layer 3 VSN (IPv4)	128 including mgmt VRF and GRT	256 including mgmt VRF and GRT	256 including mgmt VRF and GRT
SPB-PIM Gateway controller S,Gs (source announcements) with MSDP (IPv4)	6,000	6,000	6,000
SPB-PIM Gateway controllers per SPB fabric (IPv4)	5	5	5
SPB-PIM Gateway nodes per SPB fabric (IPv4)	64	64	64
SPB-PIM Gateway interfaces per BEB (IPv4)	64	64	64
PIM neighbors per SPB-PIM Gateway node (IPv4)	64	64	64
Distributed Virtual Routing (DvR)			
DvR Virtual IP interfaces	n/a	501 with vIST 502 without vIST	501 with vIST 502 without vIST
DvR domains per SPB fabric	n/a	16	16
Controller nodes per DvR domain	n/a	8	8
Leaf nodes per DvR domain	n/a	250	250
DvR enabled Layer 2 VSNs	n/a	501 with vIST 502 without vIST	501 with vIST 502 without vIST
DvR host route scaling	n/a	32,000	32,000

Table continues…

	Maximum number supported		
	VSP 4000 Series	**VSP 7200 Series**	**VSP 8000 Series**
✱ **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.			
VXLAN Gateway			
MAC addresses in base interworking mode	n/a	112,000	112,000
MAC addresses in full interworking mode	n/a	74,000	74,000
VNI IDs per node	n/a	2,000	2,000
VTEP destinations per node or VTEP	n/a	500	500
Filters, QoS, and Security			
Total IPv4 Ingress rules/ ACEs (Port/VLAN based, Security/QoS filters)	1,530	766	766
Total IPv4 Egress rules/ ACEs (Port based, Security filters)	254	252	252
Total IPv6 Ingress rules/ ACEs (Port/VLAN based, Security/QoS filters)	256	256	256
EAPoL 802.1x (clients per port)	32	32	32
OAM and Diagnostics			
FTP sessions (IPv4/IPv6)	4	4	4
Rlogin sessions (IPv4/ IPv6)	8	8	8
SSH sessions (IPv4/IPv6)	8 total (any combination of IPv4 and IPv6)	8 total (any combination of IPv4 and IPv6)	8 total (any combination of IPv4 and IPv6)
Telnet sessions (IPv4/ IPv6)	8	8	8
Mirrored ports	49	53 (up to 71 with channelization)	83 (up to 95 with channelization)
Fabric RSPAN Port mirror instances per switch (Ingress only)	Port mirror sessions can be mapped to a maximum of 24 unique I-SID offsets for Ingres Mirror. Only one I-SID offset for Egress Mirror.	Port mirror sessions can be mapped to a maximum of 24 unique I-SID offsets for Ingres Mirror. Only one I-SID offset for Egress Mirror.	Port mirror sessions can be mapped to a maximum of 24 unique I-SID offsets for Ingres Mirror. Only one I-SID offset for Egress Mirror.

Table continues…

	Maximum number supported		
	VSP 4000 Series	**VSP 7200 Series**	**VSP 8000 Series**
Fabric RSPAN Flow mirror instances per switch (Ingress only)	Filter ACL ACE sessions can be mapped to only 1 mirror I-SID offset.	Filter ACL ACE sessions can be mapped to a maximum of 24 unique I-SID offsets.	Filter ACL ACE sessions can be mapped to a maximum of 24 unique I-SID offsets.
Fabric RSPAN Monitoring ISIDs (network value)	1000 Monitoring I-SIDs across SPB network.	1000 Monitoring I-SIDs across SPB network.	1000 Monitoring I-SIDs across SPB network.
sFlow sampling limit	100 samples per second	3,000 samples per second	3,000 samples per second

The following table provides information on IPv4 and IPv6 route scaling.

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 2: IPv4 and IPv6 route scaling

URPF mode	IPv6 mode	VSP 4000 Series			VSP 7200 Series and VSP 8000 Series		
		IPv4	IPv6		IPv4	IPv6	
			Prefix less than 64	Prefix greater than 64		Prefix less than 64	Prefix greater than 64
No	No	15,744	7,887	256	15,488	7,744	n/a
No	Yes	n/a	n/a	n/a	7,488	3,744	2,000
Yes	No	7,744	3,872	256	7,488	3,744	n/a
Yes	Yes	n/a	n/a	n/a	3,488	1,744	1,000

VRF scaling note

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 3999) for internal use.

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

Fabric scaling for VSP 4000 Series

The following table provides fabric scaling information.

Table 3: Fabric scaling

Attribute	vIST configured	vIST not configured
Number of SPB regions	1	1
Number of B-VIDs	2	2
Maximum number of Physical and Logical (Fabric Extend) NNI interfaces/adjacencies	VSP 4450 = 255 VSP 4850 = 24	VSP 4450 = 255 VSP 4850 = 24
SPBM enabled switches per region (BEB + BCB)	500	500
Number of BEBs this node can share services with (Layer 2 VSNs, Layer 3 VSNs, E-Tree, Multicast, Transparent Port UNI). vIST clusters are counted as 3 nodes. Each Fabric Extend ISIS adjacency or VXLAN remote VTEP reduces this number by 1.	500	500
Maximum number of vIST/IST clusters this node can share I-SIDs with	500	500
Layer 2 MAC table size (with SPBM)	16,000	16,000
I-SIDs supported	See Table 4: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 35.	See Table 4: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 35.
Maximum number of Layer 2 VSNs per switch	1,000	1,000
Maximum number of Switched UNI I-SIDs per switch	See Table 4: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 35.	See Table 4: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 35.
Maximum number of Transparent Port UNIs per switch	48	48
Maximum number of E-Tree PVLAN UNIs per switch	1,000	1,000
Maximum number of Layer 3 VSNs per switch	128 including mgmt VRF and GRT	128 including mgmt VRF and GRT
Maximum number of SPB Layer 2 multicast UNI I-SIDs	See Table 4: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 35.	See Table 4: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 35.

Table continues…

Attribute	vIST configured	vIST not configured
Maximum number of SPB Layer 3 multicast UNI I-SIDs	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.	
Maximum number of FA ISID/ VLAN assignments per port	94	94
Maximum number of IP multicast S,Gs when operating as a BCB	1,000	1,000

Table 4: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs)

Number of IS-IS interfaces (NNIs)	vIST configured	vIST not configured
4	1,000	1,000
6	1,000	1,000
10	650	1,000
20	350	700
48	n/a	n/a
72	n/a	n/a
100	n/a	n/a
128	n/a	n/a
250	n/a	n/a

Fabric scaling for VSP 7200 Series

The following table provides fabric scaling information.

Table 5: Fabric scaling

Attribute	vIST configured	vIST not configured
Number of SPB regions	1	1
Number of B-VIDs	2	2
Maximum number of Physical and Logical (Fabric Extend) NNI interfaces/adjacencies	255	255
SPBM enabled switches per region (BEB + BCB)	500	500
Number of BEBs this node can share services with (Layer 2	500	500

Table continues…

Attribute	vIST configured	vIST not configured
VSNs, Layer 3 VSNs, E-Tree, Multicast, Transparent Port UNI). vIST clusters are counted as 3 nodes. Each Fabric Extend ISIS adjacency or VXLAN remote VTEP reduces this number by 1.		
Maximum number of vIST/IST clusters this node can share I-SIDs with	330	330
Layer 2 MAC table size (with SPBM)	112,000	112,000
I-SIDs supported	See Table 6: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 37.	See Table 6: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 37.
Maximum number of Layer 2 VSNs per switch	4,059	4,059
Maximum number of Switched UNI I-SIDs per switch	See Table 6: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 37.	See Table 6: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 37.
Maximum number of Transparent Port UNIs per switch	54 (up to 72 with channelization)	54 (up to 72 with channelization)
Maximum number of E-Tree PVLAN UNIs per switch	4,059	4,059
Maximum number of Layer 3 VSNs per switch	256 including mgmt VRF and GRT	256 including mgmt VRF and GRT
Maximum number of SPB Layer 2 multicast UNI I-SIDs	See Table 6: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 37.	See Table 6: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 37.
Maximum number of SPB Layer 3 multicast UNI I-SIDs	Maximum 6000 for a BEB: Due to internal resource sharing IP Multicast scaling depends on network topology. Switch will issue warning when 85 and 90% of available resources are reached.	
Maximum number of FA ISID/ VLAN assignments per port	94	94
Maximum number of IP multicast S,Gs when operating as a BCB	16,000	16,000

Table 6: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs)

Number of IS-IS interfaces (NNIs)	vIST configured	vIST not configured
4	4,000	4,000
6	3,500	4,000
10	2,900	4,000
20	2,000	4,000
48	1,000	2,000
72	750	1,500
100	550	1,100
128	450	900
250	240	480

Fabric scaling for VSP 8000 Series

The following table provides fabric scaling information.

Table 7: Fabric scaling

Attribute	vIST configured	vIST not configured
Number of SPB regions	1	1
Number of B-VIDs	2	2
Maximum number of Physical and Logical (Fabric Extend) NNI interfaces/adjacencies	255	255
SPBM enabled switches per region (BEB + BCB)	500	500
Number of BEBs this node can share services with (Layer 2 VSNs, Layer 3 VSNs, E-Tree, Multicast, Transparent Port UNI). vIST clusters are counted as 3 nodes. Each Fabric Extend ISIS adjacency or VXLAN remote VTEP reduces this number by 1.	500	500
Maximum number of vIST/IST clusters this node can share I-SIDs with	330	330
Layer 2 MAC table size (with SPBM)	112,000	112,000

Table continues…

Attribute	vIST configured	vIST not configured
I-SIDs supported	See Table 8: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 38.	See Table 8: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 38.
Maximum number of Layer 2 VSNs per switch	4,059	4,059
Maximum number of Switched UNI I-SIDs per switch	See Table 8: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 38.	See Table 8: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 38.
Maximum number of Transparent Port UNIs per switch	84 (up to 96 with channelization)	84 (up to 96 with channelization)
Maximum number of E-Tree PVLAN UNIs per switch	4,059	4,059
Maximum number of Layer 3 VSNs per switch	256 including mgmt VRF and GRT	256 including mgmt VRF and GRT
Maximum number of SPB Layer 2 multicast UNI I-SIDs	See Table 8: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 38.	See Table 8: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs) on page 38.
Maximum number of SPB Layer 3 multicast UNI I-SIDs	Maximum 6000 for a BEB: Due to internal resource sharing IP Multicast scaling depends on network topology. Switch will issue warning when 85 and 90% of available resources are reached.	
Maximum number of FA ISID/ VLAN assignments per port	94	94
Maximum number of IP multicast S,Gs when operating as a BCB	16,000	16,000

Table 8: Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs)

Number of IS-IS interfaces (NNIs)	vIST configured	vIST not configured
4	4,000	4,000
6	3,500	4,000
10	2,900	4,000
20	2,000	4,000
48	1,000	2,000
72	750	1,500
100	550	1,100

Table continues…

Number of IS-IS interfaces (NNIs)	vIST configured	vIST not configured
128	450	900
250	240	480

Recommendations

This section provides recommendations that affect feature configuration.

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

VSP 7200 and 8000 Series

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

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

VSP 4000 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.

File names for this release

This section lists the software files for the following VOSS platforms:

- VSP 4000 Series
- VSP 7200 Series
- VSP 8000 Series

⚠ **Caution:**

To download the software files, use Mozilla Firefox. Do not use Internet Explorer or Google Chrome to download software files.

Download images using the binary file transfer.

Check that the file type suffix is `.tgz` and that the image names after you download them to the device match those shown in the following table. Some download utilities append `.tar` to the file name or change the filename extension from `.tgz` to `.tar`. If the file type suffix is `.tar` or the filename does not exactly match the names shown in the preceding table, rename the downloaded file to the name shown in the table so that the activation procedures operate properly.

Important:

After you download the software, calculate and verify the md5 checksum. To calculate and verify the md5 checksum on the device, see Calculating and verifying the md5 checksum for a file on a switch on page 41. To calculate and verify the md5 checksum on a Unix or Linux machine, see Calculating and verifying the md5 checksum for a file on a client workstation on page 42. On a Windows machine, use the appropriate Windows utility that is supported on your Windows version.

Starting in VOSS 4.2, the encryption modules are included as part of the standard runtime software image file.

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

The following table lists the files for this release.

Table 9: VSP 4000 file names and sizes

Description	File name	Size (in bytes)
Standard runtime software image	VOSS4K.6.0.1.0.tgz	101,359,539
MIB files	• VOSS4K.6.0.1.0_mib.zip • VOSS4K.6.0.1.0_mib.txt	• 1,049,978 • 6,973,514
Supported MIB object names	VOSS4K.6.0.1.0_mib_sup.txt	1,074,135
EDM Help	VSP4000v601_HELP_EDM_gzip.zip	3,334,694
EDM plug-in for COM	VSP4000v6.0.1.0.zip	4,860,560
Logs reference	VOSS4K.6.0.1.0_edoc.tar	61,224,960

Table 10: VSP 7200 file names and sizes

Description	File name	Size (in bytes)
Standard runtime software image	VOSS7K.6.0.1.0.tgz	64,983,023
MIB files	• VOSS7K.6.0.1.0_mib.zip • VOSS7K.6.0.1.0_mib.txt	• 1,049,978 • 6,973,514
Supported MIB object names	VOSS7K.6.0.1.0_mib_sup.txt	1,076,265
EDM Help	VOSSv601_HELP_EDM_gzip.zip	3,343,282
EDM plug-in for COM	VOSSv6.0.1.0.zip	5,398,524
Logs reference	VOSS7K.6.0.1.0_edoc.tar	61,224,960

Table 11: VSP 8000 file names and sizes

Description	File name	Size (in bytes)
Standard runtime software image	VOSS8K.6.0.1.0.tgz	64,983,867
MIB files	• VOSS8K.6.0.1.0_mib.zip • VOSS8K.6.0.1.0_mib.txt	• 1,049,978 • 6,973,514
Supported MIB object names	VOSS8K.6.0.1.0_mib_sup.txt	1,076,265
EDM Help	VOSSv601_HELP_EDM_gzip.zip	3,343,282
EDM plug-in for COM	VOSSv6.0.1.0.zip	5,398,524
Logs reference	VOSS8K.6.0.1.0_edoc.tar	61,224,960

Open Source software files

The following table lists the details of the Open Source software files distributed with the switch software.

Table 12: Open Source software files

Product	Master copyright file	Open source base software for 5.0
VSP 4000 Series	VOSS4K.6.0.1.0_oss-notice.html	VOSS4K.6.0.1.0_OpenSource.zip
VSP 7200 Series	VOSS7K.6.0.1.0_oss-notice.html	VOSS7K.6.0.1.0_OpenSource.zip
VSP 8000 Series	VOSS8K.6.0.1.0_oss-notice.html	VOSS8K.6.0.1.0_OpenSource.zip

Calculating and verifying the md5 checksum for a file on a switch

Perform this procedure on a VSP switch to verify that the software files downloaded properly to the switch. The md5 checksum for each release is available on the Extreme Networks Support website.

Before you begin

- Download the md5 checksum to an intermediate workstation or server where you can open and view the contents.
- Download the .tgz image file to the switch.

About this task

Calculate and verify the md5 checksum after you download software files.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Use the **ls** command to view a list of files with the `.tgz` extension:

   ```
   ls *.tgz
   ```

3. Calculate the md5 checksum for the file:

```
md5 <filename.tgz>
```

4. Compare the number generated for the file on the switch with the number that appears in the md5 checksum on the workstation or server. Ensure that the md5 checksum of the software suite matches the system output generated from calculating the md5 checksum from the downloaded file.

Example

The following example provides output for VSP 8200 but the same process can be used on other VSP switches.

View the contents of the md5 checksum on the workstation or server:

```
3242309ad6660ef09be1b945be15676d  VSP8200.4.0.0.0_edoc.tar
d000965876dee2387f1ca59cf081b9d6  VSP8200.4.0.0.0_mib.txt
897303242c30fd944d435a4517f1b3f5  VSP8200.4.0.0.0_mib.zip
2fbd5eab1c450d1f5feae865b9e02baf  VSP8200.4.0.0.0_modules.tgz
a9d6d18a979b233076d2d3de0e152fc5  VSP8200.4.0.0.0_OpenSource.zip
8ce39996a131de0b836db629b5362a8a  VSP8200.4.0.0.0_oss-notice.html
80bfe69d89c831543623aaad861f12aa  VSP8200.4.0.0.0.tgz
a63a1d911450ef2f034d3d55e576eca0  VSP8200.4.0.0.0.zip
62b457d69cedd44c21c395505dcf4a80  VSP8200v400_HELP_EDM_gzip.zip
```

Calculate the md5 checksum for the file on the switch:

```
Switch:1>ls *.tgz
-rw-r--r--  1 0       0         44015148 Dec  8 08:18  VSP8200.4.0.0.0.tgz
-rw-r--r--  1 0       0         44208471 Dec  8 08:19  VSP8200.4.0.1.0.tgz
Switch:1>md5 VSP8200.4.0.0.0.tgz
MD5 (VSP8200.4.0.0.0.tgz) = 80bfe69d89c831543623aaad861f12aa
```

Calculating and verifying the md5 checksum for a file on a client workstation

Perform this procedure on a Unix or Linux machine to verify that the software files downloaded properly. The md5 checksum for each release is available on the Extreme Networks Support website.

About this task

Calculate and verify the md5 checksum after you download software files.

Procedure

1. Calculate the md5 checksum of the downloaded file:

   ```
   $ /usr/bin/md5sum <downloaded software-filename>
   ```

   Typically, downloaded software files are in the form of compressed Unix file archives (.tgz files).

2. Verify the md5 checksum of the software suite:

   ```
   $ more <md5-checksum output file>
   ```

3. Compare the output that appears on the screen. Ensure that the md5 checksum of the software suite matches the system output generated from calculating the md5 checksum from the downloaded file.

Example

The following example uses files from Virtual Services Platform 4000 Series but the same process applies to software files for all VSP switches.

Calculate the md5 checksum of the downloaded file:

```
$ /usr/bin/md5sum VSP4K.4.0.40.0.tgz

02c7ee0570a414becf8ebb928b398f51 VSP4K.4.0.40.0.tgz
```

View the md5 checksum of the software suite:

```
$ more VSP4K.4.0.40.0.md5
285620fdc1ce5ccd8e5d3460790c9fe1 VSP4000v4.0.40.0.zip

a04e7c7cef660bb412598574516c548f VSP4000v4040_HELP_EDM_gzip.zip
ac3d9cef0ac2e334cf94799ff0bdd13b VSP4K.4.0.40.0_edoc.tar
29fa2aa4b985b39843d980bb9d242110 VSP4K.4.0.40.0_mib_sup.txt
c5f84beaf2927d937fcbe9dd4d4c7795 VSP4K.4.0.40.0_mib.txt
ce460168411f21abf7ccd8722866574c VSP4K.4.0.40.0_mib.zip
1ed7d4cda8b6f0aaf2cc6d3588395e88 VSP4K.4.0.40.0_modules.tgz
1464f23c99298b80734f8e7fa32e65aa VSP4K.4.0.40.0_OpenSource.zip
945f84cb213f84a33920bf31c091c09f VSP4K.4.0.40.0_oss-notice.html
02c7ee0570a414becf8ebb928b398f51 VSP4K.4.0.40.0.tgz
```

Supported upgrade paths

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

Validated upgrade paths are from 5.0 or 5.1 to 6.0.1.

At the time of publishing this document, there were no known restrictions on upgrades. Customers can upgrade directly from other releases to this release. Extreme recommends that for non-validated upgrade paths, users perform the upgrade with one or two switches initially before a widespread upgrade.

Unless specifically stated otherwise, the information in this section applies to all VOSS platforms.

Upgrading DvR configuration from 6.0.1.0 or 6.0.1.1 to 6.1.1.0

Use the following process to upgrade the DvR configuration.

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 6.1.1.0 on the Controllers, and then reboot the Controllers.

To upgrade DvR Leaf nodes:

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

   Important:

   Do not save the configuration.
3. Upgrade the software to 6.1.1.0 on the Leaf nodes, and then reboot the nodes.

TACACS+ upgrade consideration

When you upgrade from VOSS 4.1.X to VOSS 4.2 or a higher release, the TACACS+ host configurations will be lost. After the upgrade, the TACACS+ host configurations will not take effect so you must reconfigure them. After you make the configurations, you must save the changes on the device. You should also save the configuration to a file to retain the configuration settings.

Note:

This issue affects upgrades from VOSS 4.1.X only. It does not affect upgrades from VOSS 4.2 or higher.

Best practices for SPB regarding MSTP

Use NNI ports exclusively to transport traffic for SPB-based services and not be configured as members of any VLANs other than SPB B-VLANs. In releases that do not support nni-mstp, when an SPBM IS-IS interface is created on an NNI port or an MLT, MSTP is automatically disabled for MSTI-62 on the port/MLT. However, MSTP is not automatically disabled on NNI ports for the CIST (default MSTI). In releases that support the **`boot config flags nni-mstp`** command, the default behavior of the MSTP NNI ports is that CIST is disabled automatically on the NNI and the NNI ports cannot be members of any VLANs other than B-VLANs. The default boot config flags nni-mstp must be set to false (which is the default). The following example shows the command to disable the MSTP on the NNI ports.

Example:

```
Switch:1(config)#interface gigabitEthernet 1/8
Switch:1(config-if)#no spanning-tree mstp
```

Coexistence of MSTP and SPB-based services on NNI ports

In releases that do not support nni-mstp boot configuration, you can support the coexistence of non-SPB based services on the NNI ports, by adding NNI ports as members of VLANs, except for B-VLANs. These other VLANs rely on the use of MSTP for Loop prevention. The network operator must carefully consider the implications of keeping MSTP enabled on the NNI ports because any MSTP topology changes detected on the NNI ports impacts all services and causes most dynamically learned information on the UNI side to be flushed and relearned. This includes, but is not limited to, all customer MAC and ARP records. This can also cause all the UNI ports on a BEB to be temporarily put into a spanning-tree blocking state before transitioning to a forwarding state again. The net result is that MSTP topology changes on the NNI ports adversely impact traffic for SPB-based services. Therefore, it is recommended that the NNI ports be used exclusively for SPB traffic.

If you upgrade to a release that supports the mstp default behavior change that is associated with the boot config flags nni-mstp, and your previous configuration included coexistence of MSTP and SPB-based services on the NNI ports in the configuration file, take note of the following:

During startup, your configuration file continues to load successfully but now it includes a change that sets the nni-mstp flag to true (if it was not already set to true). Your system operates the same as before the upgrade.

After startup, save the configuration file. If you do not save your configuration, you continue to see the following message on reboot.

```
Warning
Detected brouter and/or vlans other than BVLANs on NNI ports. Setting the boot config
flag nni-mstp to true. Saving configuration avoids repetition of this warning on reboot.
```

For information about upgrading, see *Administering*.

For information about feature support, see *Release Notes*.

Feature licensing

After you start a new system, the 60–day Premium Trial license countdown begins. You will see notification messages as the countdown approaches the end of the trial period. After 60 days, the Premium Trial license expires. You will see messages on the console and in the alarms database that the license has expired. The next time you restart the system after the license expiration, the system no longer supports Premier services.

If you use a Base License, you do not need to install a license file. If you purchase a Premier License, you must obtain and install a license file. For more information about how to install a license file, see *Administering*.

Important:

The license filename stored on a device must meet the following requirements:

- Maximum of 63 alphanumeric characters
- No spaces or special characters allowed

- Underscore (_) is allowed
- The file extension ".xml" is required

SFP+ ports

SFP+ ports support 1 Gbps and 10 Gbps transceivers only.

For a complete list of supported SFPs and QSFPs, see *Installing Transceivers and Optical Components on VSP Operating System Software*, NN47227-301.

show vlan remote-mac-table command output

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

Because all MinM packets that originate from the IST switch use the virtual B-MAC as the source B-MAC, 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.

dos-chkdsk

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

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

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

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.

Interoperability notes for Fabric Attach

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

Table 13: Extending Fabric using Static FA Proxy configuration (ISID/VLAN is manually configured on FA Proxy)

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

Table 14: Extending Fabric to FA Clients by using FA Proxy

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

Note:

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

Interoperability considerations for IS-IS external metric

Support for the `external` metric in IS-IS has been added in VOSS release 5.0. BEBs running VOSS 5.0 can advertise routes into IS-IS with the metric type as external. They can also correctly interpret routes advertisements with metric type external received via IS-IS. In an SPB network with a mix of product types running different versions of software releases, care must to be taken to ensure that turning on the ability to use metric-type external does not cause unintended loss of connectivity.

Important:

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 L3VSN enabled. For example, this applies to L2 only BEBs and BCBs.
- There are no special release or product type implications if the L3VSN 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`, irrespective of the metric-type (internal or external) used by the advertising BEB in its route advertisement.
- Switches running VSP 9000 release 4.1.0.0 or later will treat all IS-IS routes as having metric-type `internal`, irrespective of the metric-type (internal or external) used by the advertising BEB in its route advertisement.
- Switches running VOSS releases prior to 4.2.1.0 may not correctly install IS-IS routes in a L3VSN if any routes are advertised with metric-type external are advertised in that L3VSN by other BEBs in the network. L3VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to GRT.
- Switches running VSP 9000 releases prior to 4.1.0.0 may not correctly install IS-IS routes in a L3VSN if any routes are advertised with metric-type external are advertised in that L3VSN by other BEBs in the network. L3VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to GRT.
- Switches running any ERS 8800 release may not correctly install IS-IS routes in of a L3VSN if any routes are advertised with metric-type external are advertised in that L3VSN by other BEBs in the network. L3VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to GRT.

VSP 4000 specific notices

Converting ERS 4850 to VSP 4000

This section lists information on Extreme Networks switch conversion supported in this release.

Important:

Switch conversion is applicable only to the Virtual Services Platform 4000 Series. Currently, only the conversion of an ERS 4850 switch to a VSP 4000 switch is supported.

Interoperability notes for VSP 4000 connecting to an ERS 8800

- For customers running 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 the minimum software version is 7.1.5.4. The “spbm version” on the ERS 8800 must be set to “802.1aq”.
- For customers running 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 the minimum software version is 7.2.1.1.
- Diffserv is enabled in the VSP 4000 port settings, and is disabled in the ERS 8800 port settings, by default.

Notes on combination ports for VSP 4000

When the VSP 4000 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 are applicable 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 peer switch to disable auto-negotiation.

Chapter 4: Known issues and limitations

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

Known issues in this release

This section identifies the known issues in this release for the following products:

- VSP 4000 Series
- VSP 7200 Series
- VSP 8000 Series

Device related issues

Table 15: Known issues

Issue number	Description	Workaround
wi01144867	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`.
wi01166763	SLA Mon tests fail (between 2% and 8% failure) between VSP 4000 devices when you have too many agents involved with scaled configurations.	This happens only in a scaled scenario with more than seven agents, otherwise the failure does not occur. The acceptable failure percentage is 5%, but you may see failures of up to 8%.
wi01168610	VSP 4450GSX: The command **sys shutdown** does not change the STATUS LED on the VSP 4450GSX-PWR+ device.	None. This issue does not impact any functionality.
wi01168706	The following error message occurs on VSP 4000 when performing **shutdown/no-shutdown** commands continuously: `IO1 [05/02/14 06:59:55.178:UTC] 0x0011c525 00000000 GlobalRouter COP-SW ERROR vsp4kTxEnable Error`	None. When this issue occurs, the port in question may go down, then performs a **shutdown/no-shutdown** of the port to bring it up and resumes operation.

Table continues…

Issue number	Description	Workaround
	`changing TX disable for SFP module: 24, code: -8`	
wi01171802	VSP 4450GSX: On a fresh boot, peer ports connected to ports 1/49 and 1/50 bounce and may cause additional transitions in the network.	None.
wi01171907	VSP 4450GSX: CAKs are not cleared after setting VSP 4000 to factory-default.	None. Currently this is the default behavior and does not affect functionality of the MACsec feature.
wi01173026	A reboot with verbose configuration does not allow you to delete a VRF.	This issue occurs only if you save the configuration file in verbose mode and reboot the switch in that configuration. This situation is unlikely to exist; verbose mode is used more as a diagnostic tool. This issue does not impact functionality.
wi01173136	T1 SFP: Shutting down the T1 link from one end of the VSP 4000 or VSP 7200 Series or VSP 8000 Series does not shut down the link at the remote end. You may experience traffic loss if the remote side of the link is not shut down.	This issue occurs only when a T1 SFP link from one end is shutdown. Enable a dynamic link layer protocol such as LACP or VLACP on both ends to shut the remote end down too. As an alternative, administratively disable both ends of the T1 SFP link to avoid the impact.
wi01175118	On a MACsec enabled port, you may see delayed packets when the MACsec port is kept running for more than 12 hours. This delayed packet counter may 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.
wi01195988	You cannot use EDM to issue ping or traceroute commands for IPv6 addresses.	Use CLI to initiate ping and traceroute.
wi01196000	You cannot use EDM to issue ping or traceroute commands for IPv4 addresses.	Use CLI to initiate ping and traceroute.
wi01197712	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.

Table continues…

Issue number	Description	Workaround
	Note: This issue is specific to VSP8404QQ ESMs.	
wi01208650	The Console gets disconnected frequently when you enable screen trace (trace screen enable). The error displayed is `Forced log-out after 65535 secs`.	None
wi01209346	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. • The Indiscard packet count gets incremented on the **`show int gig error`** statistics command.	Use a v3 interface as querier in a LAN segment which has snoop– enabled v2 and v3 interfaces.
wi01209604	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 perform a Layer 2 IP PING.
wi01210104	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. **Note:** This issue applies to products that support 40 Gbps ports.	None.
wi01212099	In the COM EDM Plugin command, the Layer 2 Traceroute IPv6 does not work properly and gives the error, `No Such Name`.	Use the CLI to initiate the Layer 2 Traceroute for IPv6.
wi01212115	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.
wi01212860	An intermittent link-flap issue can occur in the following circumstance for the copper ports of	Administratively shutdown, and then reenable the port.

Table continues…

Issue number	Description	Workaround
	the VSP 7254XTQ or the 8424XT ESM for VSP 8400: 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.	**Note:** Extreme recommends that you use auto-negotiation. Disabling auto-negotiation on these ports is not a recommended configuration.
wi01214025	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.
wi01214772	The 4 byte AS confederation identifier and peers configuration are not retained across a reboot. This problem occurs when 4 Byte AS is enabled with confederation.	Reconfigure the 4 byte AS confederation identifier and peers on the device, and reboot.
wi01215220	After you enable enhanced secure mode, and log in for the first time, the system prompts you to enter a new password. If you do not meet the minimum password requirements, the following system output message appears: `Password should contain a minimum of 2 upper and lowercase letters, 2 numbers and 2 special characters like !@#$%^*(). Password change aborted. Enter the New password:` The system output message does not display the actual minimum password requirements you need to meet, which are configured on your system. The output message is an example of what the requirements may need to meet. The actual minimum password requirements you need to meet are configured on your system by the administrator.	None.
wi01215773	The switch provides an NTP log message that indicates that the NTP server did not synchronize, even though one of the NTP servers synchronized correctly and the NTP stats show that it did.	None.
wi01216535	The `router ospf` entry always appears in the configuration file regardless of whether	None.

Table continues…

Issue number	Description	Workaround
	OSPF is configured. This line does not perform any configuration and has no impact on the running software.	
wi01216550	When you use Telnet or SSH to connect to the switch, it can take up to 60 seconds for the login prompt to appear. However, this situation is very unlikely to happen, and it does not appear in a standard normal operational network.	Do not provision DNS servers on a switch to avoid this issue altogether.
wi01217251	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.
wi01217347	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.
wi01217871	If you attach the QSFP+ end of a passive breakout cable to a VSP 4000 or VSP 7200 Series or VSP 8000 Series switch, and the SFP+ ends of the cable to a VSP 9000 running Release 4.0.1, the output for the **`show pluggable-optical-modules basic`** command on the VSP 9000 shows an incorrect vendor name and part number. The incorrect information also appears in EDM under the **Edit** > **Port** > **General** menu path.	This issue will be fixed in a future VSP 9000 software release.
wi01221817	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.
wi01222078	If you delete the SPBM configuration and re-configure SPBM using the same nickname but a different ISIS system id without rebooting, the switch displays an error message.	Reboot the switch after you delete the SPBM configuration.
wi01223719	You cannot use EDM to configure SSH rekey and enable or disable SFTP.	Use CLI to configure SSH rekey and enable or disable SFTP.
wi01223723	EDM displays the user name as Admin, even though you login using a different user name.	None.
wi01223759	You cannot use EDM to view the IPv6 DHCP relay counters.	Use CLI to view the IPv6 DHCP relay counters.
wi01224076	When you re-enable insecure protocols in the CLI SSH secure mode, the switch does not display a warning message.	None.

Table continues…

Issue number	Description	Workaround
wi01224644	EDM displays the IGMP group entry that is learnt on vIST MLT port is as TX-NNI.	Use CLI to view the IGMP group entry learnt on vIST MLT port.
wi01224710 VOSS-1420	On a VSP 4000 Series untagged ARP packet, ingressing on a Layer 2 VSN interface will honor default the port QOS. Changing port QOS value will not be honored.	Create an ACL filter that can remark the packet to any Queues.
wi01225023	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 default VLAN and displays an error message. This issue has no impact.	The error message is incorrect and can be ignored.
wi01225232	When an operational SMLT is removed from a TUNI ISID and is not added to any other VLAN or TUNI ISID, then spanning tree is enabled on this SMLT interface. Spanning tree is disabled when added to VLAN or TUNI ISID. This issue has no impact.	Disable SMLT ports and then remove them from TUNI ISID.
wi01225310	When ISIS is disabled on one of the VIST peer nodes with RSMLT interfaces and it has ECMP routes with the RSMLT Peer as the next hop, the ECMP routes that are being replaced during the transition of the ISIS state now will have a next hop of the local interface. This results in an error message `COP-SW ERROR ercdProcIpRecMsg: Failed to Replace IP Records`.	Enable ISIS on both the vIST peers.
wi01225514	On a VSP 7200 Series 40 Gbps ports with CR4 direct attach cables (DAC), when you manually enable or disable ISIS, the port bounces once.	Configure ISIS during the maintenance period. Bring the port down, configure the port and then bring the port up.
wi01226335	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.
wi01226433 wi01226437	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 L3 VSNs can be configured`.	None.

Table continues…

Issue number	Description	Workaround
wi01230533 wi01230953 wi01232817	When you use Fabric Extend over IP (FE-IP) and Fabric Extend over L2 VLAN (FE-VID) solution, if you change the ingress and egress .1p map, packets may not follow correct internal QoS queues for FE tunnel to FE tunnel, or FE tunnel to regular NNI traffic. .	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
wi01232095	EDM and CLI show different local preference values for a BGP IPv6 route. EDM displays path attributes as received and stored in the BGP subsystem. If the attribute is from an eBGP peer, the local preference appears as zero. CLI displays path attributes associated with the route entry, which can be modified by a policy. If a route policy is not configured, the local preference shows the default value of 100.	None
wi01232581	You cannot use EDM to enable or disable ASG. You can only view ASG status.	Use CLI to enable or disable ASG.
wi01233201	If the I-SID associated with a Switched UNI or Fabric Attach port does not have a platform VLAN association and you disable Layer 2 Trusted, then the non IP traffic coming from that port does not take the port QoS and still uses the .1p priority in the packet.	None
wi01233828 VOSS-1487	If you establish an SSH connection to a switch, and then use that switch to create a Telnet session with another device, when you exit the Telnet session, the original SSH connection can stop responding.	Halt the original SSH connection and reconnect.
wi01234422	If you improperly close an SSH session, the session structure information does not clear and the client can stop functioning.	Disable and enable SSH.
wi01234071	You cannot use EDM to clear Fabric Attach statistics for VSP 4000 Series.	Use the CLI `clear fa stats` command.
wi01234623	VSP 7200 Series and VSP 8000 Series do not Support Fabric Extend over Layer 2 VLAN (FE-VID) logical interface configuration over an MLT interface.	None
wi01234739	If you apply an ipv6-out-route-map on a BGP peer to filter a particular IPv6 prefix range with a match network condition, it does not filter the full prefix range.	Configure the incoming policy to filter incoming advertised routes on BGP+ peers.

Table continues…

Issue number	Description	Workaround
wi01234872	The **`show debug-file all`** command is missing on VSP 7200 Series and VSP 8000 Series platforms.	None
wi01234873	The system does not generate a log message, either in the log file or on screen, when you run the **`flight-recorder`** command.	None
wi01235018	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.
wi01235053	If you use EDM to create an ACL filter, the ACL tab does not automatically refresh to show the new filter.	Click **Refresh** on the ACL tab to force a data refresh.

wi01235140	You cannot configure an untagged-traffic ELAN endpoint and enable BPDU in the same command.	1. Create the untagged-traffic endpoint first:
		`untagged-traffic port {slot/port[/sub-port][-slot/port[/sub-port]][,...]`
		OR
		`untagged-traffic mlt <1-512>`
		2. Enable BPDU:
		`untagged-traffic port {slot/port[/sub-port][-slot/port[/sub-port]][,...] bpdu enable`
		OR
		`untagged-traffic mlt <1-512> bpdu enable`

VOSS-1706	EAPOL: Untagged traffic not honouring port QOS for Layer 2 trusted/ Layer 3 untrusted. Issue is only seen on EAPOL enabled port.	None
VOSS-1747	On a VSP 8404 with MLT on 10G ports on an 8424XT or 8424XTQ module, multiple VLANs that have the MLT as a member of the VLAN,	None

Table continues…

Issue number	Description	Workaround
	there is a possibility that a copy of the IP multicast traffic may not be sent on all VLANs that have a receiver on the MLT.	
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 below error messages is seen when you “shut” and “no shut” the MLT interface with ECMP, BGP+ enabled.
	Error message:`CP1 [01/23/16 11:10:16.474:UTC] 0x00108628 00000000 GlobalRouter RCIP6 ERROR rcIpReplaceRouteNotifyIpv6:FAIL ReplaceTunnelRec conn_id 2`
	`CP1 [12/09/15 12:27:02.203:UTC] 0x00108649 00000000 GlobalRouter RCIP6 ERROR ifyRpcOutDelFibEntry: del FIB of Ipv6Route failed with 0: ipv6addr: 201:6:604:0:0:0:0:0, mask: 96, nh: 0:0:0:0:0:0:0:0 cid 6657 owner BGP`
	`CP1 [12/09/15 12:20:30.302:UTC] 0x00108649 00000000 GlobalRouter RCIP6 ERROR ifyRpcOutDelFibEntry: del FIB of Ipv6Route failed with 0: ipv6addr: 210:6:782:0:0:0:0:0, mask: 96, nh: fe80:0:0:0:b2ad:aaff:fe55:5088 cid 2361 owner OSPF`
		Disable the alternate path.

VOSS-2036	IPsec statistics for the management interface do not increment for **inESPFailures** or **InAHFailures**.	None.
VOSS-2117	If you configure static IGMP receivers on an IGMPv3 interface and a dynamic join and leave are received on that device from the same destination VLAN or egress point, the device stops forwarding traffic to the static receiver group after the dynamic leave is processed on the device. The end result is that the IGMP static groups still exist on the device but traffic is not forwarded.	Disable and re-enable IGMP Snooping on the interface.

Table continues…

Issue number	Description	Workaround
VOSS-2128	EAP Security and Authentication tabs displays 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 CLI command. "show eapol port interaface" to get 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 L2 traceroute between two BEB's via a transit BCB, transit BCB's hop is not seen, if the transit BCB has **ISIS adjacencies over FE l3core with both** source BEB and destination BEB.	None
VOSS-2253	Trace level command does not list module IDs when '?' is used.	To get the list of all module IDs, type "trace level" and then press Enter.
VOSS-2270 wi01227920 wi01230534	The packet internal CoS is derived incorrectly for packets sourced from a brouter port when the CoS should be derived from the port level QoS. The following list identifies scenarios that derive the internal CoS from the port QoS: • Untagged non-IP packet • Untagged IP packet, and the source port is Layer 3 untrusted • Tagged non-IP packet and the source port is Layer 2 untrusted • Tagged IP packet and the source port is Layer 3 untrusted and Layer 2 untrusted.	Use the port default QoS configuration for the brouter port. The port default configuration is Layer 2 trusted and Layer 3 trusted, and under this configuration, only the first scenario in the list is still an issue. The other scenarios do not occur.
VOSS-2279	When IPv6 neighbor device boots up, the following error message occurs in the peer device console: `GlobalRouter COP-SW ERROR ercdProcIpv6RouteMsg: Failed to Delete IPV6 Record - Ip: fe80:0:0:8dc:b2ad:aaff:fe55:1b91, NextHop:0:0:0:0:0:0:0:0, mask: 128`	There is no functional impact. Port shut/no shut which recovers the traffic works even when the switch is in error state.
VOSS-2285	When on BEB, continuously pinging IPv6 neighbor address using CLI command ping -s, ping packets don't drop, but see "no answer" messages.	Restart the ping. Avoid intensive CPU processing.

Table continues…

Issue number	Description	Workaround
VOSS-2333	L2 ping to Virtual BMAC (VBMAC) fails, if the VBMAC is reachable via L2core.	None
VOSS-2397	If you configure a channelized port in EDM by using the **Configuration > Edit > Port > General** or **Configuration > Edit > Port > IP** or **IPv6** navigation paths, you can only see and configure the first sub-port.	In the **Device Physical View**, right-click the port and use the **General**, **IP**, or **IPv6** sub-menu to configure all sub-ports.
VOSS-2411	On a VSP 4450GSX-DC device, the https-port info is not displayed or saved into the config.	None
VOSS-2415	There is no option in the "Insert V3 Interface" screen of EDM to insert a VRRP v3 interface for IPv6. The two check boxes in the screen are disabled.	There is no functional impact. EDM has two menus of IP and IPv6 and this functionality is available there along with other features.
VOSS-2422	When 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-2444	The output of the **`show ip mroute stats [group address]`** wraps to an additional line. Four columns of data are on one line and the fifth column *AverageSize* wraps to an additional line. There is also an extra line feed in the column header.	None
VOSS-2859	You cannot modify the port membership on a protocol-based VLAN using EDM after it has been created.	Use the 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-4114 VOSS-4116 VOSS-4972	You cannot use Internet Explorer 11 or Firefox 49 to connect to EDM using HTTPS.	Do not use these newer browser versions until Release 6.1.
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.

Table continues…

Issue number	Description	Workaround
VOSS-4554 VOSS-4910	The `show ip vrrp address` command does not accurately display the value of the holddown timer remaining.	None.
VOSS-4627	The **qos if-policer** allows configuration of **peak-rate** and **svc-rate** in the range 64 - 10000000 Kbps. However on 1G and 10G links, the effective policer rate is on the nearest 500 Kbps boundary (approximately), with a minimum policer rate of 500 Kbps. For example, configuring both peak-rate and svc-rate at 900 will result in an effective policer rate of 1000 (Kbps). This limitation does not apply to 10M and 100M negotiated links. On 10M and 100M links, the effective policer rate is close to any configured rate in the advertised range. **Note:** Due to a related issue, the minimum rate of 64 should not be used on any link.	On 1G and 10G links, there is no workaround for this issue. The **qos if-policer peak-rate** and **svc-rate** should be configured in 500 Kbps increments in the range 500 - 10000000.
VOSS-4728	If you remove and recreate an IS-IS instance on an NNI port with autonegotiation enabled in addition to vIST and R/SMLT enabled, it is possible that the NNI port will briefly become operationally down but does recover quickly. This operational change can lead to a brief traffic loss and possible reconvergence if non-ISIS protocols like OSPF or BGP are also on the NNI port.	If you need to remove and recreate an IS-IS instance on an autonegotiation enabled NNI port that also has non-ISIS traffic, do so during a maintenance window to minimize possible impact to other non-ISIS traffic.
VOSS-4840	If you run the `show fulltech command` in an SSH session, do not disable SSH on the system. Doing so can block the SSH session.	None.
VOSS-4843	CDP packet is sending prompt for Device ID and Platform.	None.
VOSS-4856	On a DvR Leaf, you cannot configure an sFlow agent IP address to use one of the subnets that is DvR enabled or a DvR controller.	On a DvR Leaf, configure the sFlow agent with the IP address of a brouter or management interface.
VOSS-4908	When a tunnel to a VTEP does down on a vIST peer, the MAC address is not relearned during the first mac-aging timer interval. The VTEP continues to flood traffic ensuring there is no traffic loss. The MAC address is synchronized at the next mac-aging timer trigger.	None.

Table continues…

Issue number	Description	Workaround
VOSS-4935	The system will display unnecessary `rcdRadixLookup` failed messages if you perform any of the following functions simultaneously in both vIST peers: • Delete a VLAN. • Delete ISID of a VLAN. • Disable DvR. • Reboot the switch.	None. There is no functional impact if this message appears while performing these specific actions simultaneously in both vIST peers.
VOSS-4986 VOSS-5030 VOSS-5046 VOSS-5065	You can experience MIB walk failures on the following tables: • `rcIgmpSenderTable` • `rcIsisPlsbIpUnicastFibTable` • `rcIsisPlsbMcastFibTable` • the interface table (`IF-MIB`) on a DvR leaf • `rcIpRedistributeInterVrfTable` if you use DvR and route redistribution	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-5161	If you configure a DvR Leaf for in-band management (**`inband-mgmt-ip`**), SNMP and SYSLOG protocols send out the DvR Gateway IP as the source address of packets.	To manage DvR Leaf nodes, place the management servers in a NON-DvR VLAN off a DvR Controller or on a NON-DvR I-SID off a DvR Leaf node.
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.

Limitations in this release

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

Limitations for VSP 4450GTX-HT-PWR+

⚠ **Caution:**

The VSP 4450GTX-HT-PWR+ has operating temperature and power limitations. 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 limitation or behavior and the work around, if one exists.

Table 16: Limitations for VSP 4450GTX-HT-PWR+

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.

General limitations and expected behaviors

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

Table 17: General limitations and expected behaviors

WI number	Description
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, `4k2:1(config)#isis apply redistribute direct vrf 2`.
wi01112491	IS-IS enabled ports cannot be added to an MLT. The current release does not support this configuration.
wi01122478	Stale SNMP server community entries for different VRFs appear after reboot with no VRFs . On a node with a valid configuration file saved with more than the default vrf0 , SNMP community entries for that VRF are created and maintained in a separate text file, snmp_comm.txt, on every boot. The node reads this file and updates the SNMP communities available on the node. As a result, if you boot a configuration that has no VRFs, you may still see SNMP community entries for VRFs other than the globalRouter vrf0 .
wi01137195	A static multicast group cannot be configured on a Layer 2 VLAN before enabling IGMP snooping on the VLAN. After IGMP snooping is enabled on the Layer 2 VLAN for the first time, static multicast group configuration is allowed, even when IGMP snooping is disabled later on that Layer 2 VLAN.
wi01138851	Configuring and retrieving licenses using EDM is not supported.
wi01141638	On a VSP 4000, 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.
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 greather than 1.
wi01159075	**VSP 4450GSX-PWR+**: Mirroring functionality is not working for RSTP BPDUs.
wi01171670	Telnet packets get encrypted on MACsec enabled ports.

Table continues…

WI number	Description
wi01198872	On a VSP 4000, loss of learned MAC addresses occurs in a vIST setup beyond 10k addresses. In a SPB setup the MAC learning is limited to 13k MAC addresses, due to the limitation of the internal architecture when using SPB. Moreover, as vIST uses SPB and due to the way vIST synchronizes MAC adresses 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.
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.
wi01212247	BGP tends to have many routes. Frequent additions or deletions impacts 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 blackhole in the network. Workaround: 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.
wi01213040	When you disable auto-negotiation on both sides, the 10 Gbps copper link does not come up.
wi01213066 wi01213374	EAP and NEAP are not supported on brouter ports.
wi01213336	When you configure `tx` mode port mirroring on T-UNI and SPBM NNI ports, unknown unicast, broadcast and multicast traffic packets that ingress these ports appear on the mirror destination port, although they do not egress the mirror source port. This is because `tx` mode port mirroring happens on the mirror source port *before* the source port squelching logic drops the packets at the egress port.
wi01219295	SPBM QOS: Egress UNI port does not follow port QOS with ingress NNI port & Mac-in-Mac incoming packets.
wi01219658	The command **`Show khi port-statistics`** does not display the count for NNI ingress control packets going to the CP.
wi01223526	ISIS logs duplicate system ID only when the device is a direct neighbor.

Table continues…

WI number	Description
wi01223557	Multicast outage occurs on LACP MLT when simplified vIST peer is rebooted. You can perform one of the following work arounds: • Enable PIM on the edge. • Ensure that IST peers are either RP or DR but not both.
wi01224683 wi01224689	Additional link bounce may occur on the following ports, when toggling links or during cable re-insertion: • VSP 7254XSQ 10 Gbps port • VSP 7254XSQ and VSP7254XTQ 40Gig optical cables and 40 Gbps break out cables • VSP 8200 and VSP 8400 40 Gbps ports with optical cable • VSP 8200 and VSP 8400 40 Gbps ports with optical breakout cable
wi01229417	Origination and termination of IPv6 6-in-4 tunnel is not supported on a node with vIST enabled.
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.
wi01234289	HTTP management of the ONA is not supported when it is deployed with a VSP 4000 Series device.
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.
VOSS-687	EDM and CLI show different local preference values for a BGP IPv6 route. EDM displays path attributes as received and stored in the BGP subsystem. If the attribute is from an eBGP peer, the local preference appears as zero. CLI displays path attributes associated with the route entry, which can be modified by a policy. If a route policy is not configured, the local preference shows the default value of 100.
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.
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.

Table continues…

WI number	Description
VOSS-2185	MAC move of the client to the new port does not automatically happen when you move a Non-EAP client authenticated on a specific port to another EAPoL or Non-EAP enabled port .

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 an 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*.

Note:

If you enable the ASG feature, the SSH server must use keyboard-interactive.

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

Single next hop/ARP limitation for Fabric Extend

This limitation only exists for releases that do not support VXLAN Gateway.

Default console port speed

The default console port speed for all platforms is 9600 bits per second.

Chapter 5: Resolved issues

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

Fixes from previous releases

VOSS 6.0.1 incorporates all fixes from prior releases, up to and including VOSS 5.1.1 and VOSS 6.0.

Table 18: Resolved issues in this release

Issue Number	Description
VOSS-1329	If you configure both IPv4 and IPv6 on a VLAN interface, and then change the IPv6 MTU, the IPv4 MTU is also changed for that interface.
wi01235322 VOSS-1682	Secure Copy (SCP) file transfers on VSP switches, running VOSS 5.0, stall intermittently due to 100% thread utilization of the SCP process, which is responsible for file transfer. This problem is seen intermittently when the transfer is initiated from SSH client versions earlier than OpenSSH_5.0, or for files with size of 1 GB or larger. For client versions later than OpenSSH_5.0, this stall condition is rare for file sizes up to 500 MB and has not been seen for files with sizes that are typically transferred to and from VOSS switches. The use of some older client versions such as the ones shown in the following list always result in stalled file transfers: • Sun_SSH_1.1, SSH protocols 1.5/2.0, OpenSSL 0x0090704f • OpenSSH_3.9p1, OpenSSL 0.9.7a Feb 19 2003 The recommended client and file size range to avoid this problem is to use Open SSH client version later than 5.0 and file sizes up to 500 MB.
VOSS-1758	After changing ISIS System-ID, it is possible that CFM L2 ping will not work properly.
VOSS-2237	Configuring NTP server with wrong key value, error message occurs in two scenarios. • When passwords (keys) start with a special 9 character instead of alphanumeric characters. • When passwords (keys) contain a space between characters. Error message: `setting NtpKeyTbl, Operation not allowed`
VOSS-4875	You cannot select an MLT on the **Insert Switched UNI** dialog box in EDM.

Table continues…

Issue Number	Description
VOSS-4877	If you use the `no boot config flags ?` command, `vxlan-gw-full-interworking-mode` appears as an option even though the VXLAN Gateway feature is not supported on the VSP 4000 series.
VOSS-4970	If you use the `vrfids` parameter with the `show ip msdp [count | mesh-group | peer | sa-cache | show-all | summary]` commands to display output for only a specific VRF ID or range of VRF IDs, the software displays the following error: `Info: MSDP Instance does not exist for VRF with id: 1`
VOSS-4934	Hardware fan warnings are displayed during the boot sequence of the VSP 4450GTX-HT-PWR even when no faults have occurred. Additionally, the CLI command `sys-info` does not show any info on the fan status.

Appendix A: Related information

The following section contains information related to the current release.

Overview of features by release and platform

This section provides an overview of which release introduced feature support for a particular platform. Each new release for a platform includes all the features from previous releases unless specifically stated otherwise.

Note:

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

Feature introduction

For more information about features and their configuration, see the documents listed in the respective sections.

Features	Release introduced by platform series			
	VSP 4000	**VSP 7200**	**VSP 8200**	**VSP 8400**
Default autonegotiation behavior when using a 1 Gbps SFP For more information, see the hardware documents and *Administering*	Enabled	Disabled	Disabled	N/A
Operations and management				
CLI For more information, see *Using CLI and EDM*.	3.0	4.2.1	4.0	4.2
Channelization of 40 Gbps ports For more information, see *Administering*.	N/A	4.2.1	4.2	4.2
Configuration and Orchestration Manager (COM) For more information, see Extreme Configuration and Orchestration Manager (COM) documentation.	3.0	4.2.1	4.0	4.2
Domain Name Service (DNS) client (IPv4)	3.0	4.2.1	4.0	4.2

Table continues…

Features	Release introduced by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
For more information, see *Administering*.				
DNS client (IPv6) For more information, see *Administering*.	4.1	4.2.1	4.1	4.2
The encryption modules file is included in the runtime software image file; it is not a separate file.	4.2	4.2.1	4.2	4.2
Enable or disable ICMP Broadcast/Multicast For more information, see the following documents: • *Configuring IPv4 Routing* • *Configuring IPv6 Routing*	5.1	5.1	5.1	5.1
Enable/disable IP Source Routing For more information, see the following documents: • *Configuring IPv4 Routing* • *Configuring IPv6 Routing*	5.1	5.1	5.1	5.1
Enhanced Secure mode For more information, see *Administering*.	4.2	4.2.1	4.2	4.2
Enterprise Device Manager (EDM) For more information, see *Using CLI and EDM*.	3.0	4.2.1	4.0	4.2
Entity MIB - Physical Table For more information, see *Administering*	6.0	6.0	6.0	6.0
EDM representation of physical LED status For more information, see the following documents: • *Installing Virtual Services Platform 4850GTS Series*, NN46251-300 • *Installing Virtual Services Platform 4450GTX-HT-PWR+ Switch*, NN46251–304 • *Installing Virtual Services Platform 4450GSX-PWR+ Switch*, NN46251-307 • *Installing the Virtual Services Platform 7200 Series*, NN47228-302 • *Installing the Virtual Services Platform 8000 Series*, NN47227-300	3.0	4.2.1	4.2	4.2
File Transfer Protocol (FTP) server/client (IPv4) For more information, see *Administering*.	3.0	4.2.1	4.0	4.2
FTP server/client (IPv6)	4.1	4.2.1	4.1	4.2

Table continues…

Features	Release introduced by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
For more information, see *Administering*.				
Flight Recorder (for system health monitoring) For more information, see *Troubleshooting*.	3.0	4.2.1	4.0	4.2
Forgiving mode for CWDM and DWDM SFP+ transceivers For more information, see *Installing Transceivers and Optical Components on VSP Operating System Software*, NN47227-301.	6.0	6.0	6.0	6.0
IEEE 802.1ag Connectivity Fault Management (CFM) • Layer 2 Ping • TraceRoute • TraceTree For more information, see *Configuring Fabric Connect*.	3.1	4.2.1	4.0	4.2
Industry Standard Discovery Protocol (ISDP) (CDP compatible) For more information, see *Administering*	6.0	6.0	6.0	6.0
Extensible Authentication Protocol (EAP) and EAP over LAN (EAPoL) For more information, see *Configuring Security*.	4.1	4.2.1	4.1	4.2
Extensible Authentication Protocol over LAN (EAPol) MHMA-MV For more information, see *Configuring Security*.	5.1	5.1	5.1	5.1
Link Layer Discovery Protocol (LLDP) For more information, see *Administering*	6.0	6.0	6.0	6.0
Key Health Indicator (KHI) For more information, see *Monitoring Performance*.	3.0	4.2.1	4.0	4.2
Logging (log to file and syslog [IPv4]) For more information, see *Monitoring Performance*.	3.0	4.2.1	4.0	4.2
Logging (log to file and syslog [IPv6]) For more information, see *Monitoring Performance*.	4.1	4.2.1	4.1	4.2
Mirroring (port and flow-based) For more information, see *Troubleshooting*.	3.0	4.2.1	4.0	4.2
Network Time Protocol (NTP) For more information, see *Administering*.	3.0	4.2.1	4.0	4.2

Table continues…

Features	Release introduced by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
Non EAPoL MAC RADIUS authentication For more information, see *Configuring Security*.	4.2.1	4.2.1	4.2.1	4.2.1
NTP with SHA Authentication For more information, see *Administering*.	5.1	5.1	5.1	5.1
Power over Ethernet For more information, see *Administering*.	3.0	N/A	N/A	N/A
PoE/PoE+ Allocation Using LLDP For more information, see *Administering*.	5.1	N/A	N/A	N/A
RADIUS, community-based users (IPv4) For more information, see *Configuring Security*.	3.0	4.2.1	4.0	4.2
RADIUS (IPv6) For more information, see *Configuring Security*.	4.1	4.2.1	4.1	4.2
Remote Login (Rlogin) server/client (IPv4) For more information, see *Administering*.	3.0	4.2.1	4.0	4.2
Rlogin server (IPv6) For more information, see *Administering*.	4.1	4.2.1	4.1	4.2
Remote Monitoring 1 (RMON1) for Layer 1 and Layer 2 **Note:** Release 5.0 and 5.1 do not support RMON1.	3.0	4.2.1	4.0	4.2
Remote Monitoring 2 (RMON2) for network and application layer protocols For more information, see *Monitoring Performance*.	4.2	4.2.1	4.2	4.2
Remote Shell (RSH) server/client For more information, see *Administering*.	3.0	4.2.1	4.0	4.2
Russia summer time zone change For more information, see *Administering*.	4.2	4.2.1	4.2	4.2
Secure Copy (SCP) **Note:** WinSCP client is not supported with SCP on the switch. For more information, see *Administering*.	3.0	5.0	4.0	5.0
Secure FTP (SFTP) For more information, see *Administering*.	3.0	4.2.1	4.0	4.2

Table continues…

Features	Release introduced by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
Secure hash algorithm 1 (SHA-1) and SHA-2 For more information, see *Configuring OSPF and RIP*.	4.2	4.2.1	4.2	4.2
Secure Shell (SSH) (IPv4) For more information, see *Administering*.	3.0	4.2.1	4.0	4.2
sFlow For more information, see *Monitoring Performance*.	6.0	6.0	6.0	6.0
Secure Sockets Layer (SSL) certificate management For more information, see *Administering*.	4.1	4.2.1	4.1	4.2
Simple Mail Transfer Protocol (SMTP) for log notification For more information, see the following documents: • *Monitoring Performance*	6.0	6.0	6.0	6.0
SLA Mon For more information, see *Configuring the SLA Mon Agent*.	4.1	6.0	4.1	4.2
Simple Loop Prevention Protocol (SLPP) For more information, see *Configuring VLANs, Spanning Tree, and NLB*.	3.0	4.2.1	4.0	4.2
Simple Network Management Protocol (SNMP) v1/2/3 (IPv4) For more information, see *Configuring Security*.	3.0	4.2.1	4.0	4.2
SNMP (IPv6) For more information, see *Configuring Security*.	4.1	4.2.1	4.1	4.2
SoNMP For more information, see *Administering*.	3.0	4.2.1	4.0	4.2
`spbm-config-mode` boot flag For more information, see *Configuring IP Multicast Routing Protocols*.	4.1	4.2.1	4.0.1	4.2
SSH (IPv6) For more information, see *Administering*.	4.1	4.2.1	4.1	4.2
SSH client disable For more information, see *Administering*.	6.0	6.0	6.0	6.0
SSH rekey For more information, see *Administering*.	5.1	5.1	5.1	5.1
TACACS+	4.0	4.2.1	4.1	4.2

Table continues…

Features	Release introduced by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
For more information, see *Configuring Security*.				
Telnet server/client (IPv4) For more information, see *Administering*.	3.0	4.2.1	4.0	4.2
Telnet server/client (IPv6) For more information, see *Administering*.	4.1	4.2.1	4.1	4.2
Trivial File Transfer Protocol (TFTP) server/client (IPv4) For more information, see *Administering*.	3.0	4.2.1	4.0	4.2
TFTP server/client (IPv6) For more information, see *Administering*.	4.1	4.2.1	4.1	4.2
Virtual Link Aggregation Control Protocol (VLACP) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST*.	3.0	4.2.1	4.0	4.2
Layer 2				
Switch cluster (multi-chassis LAG) - Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST*.	4.1	4.2.1	4.0	4.2
Bridge Protocol Data Unit (BPDU) Guard For more information, see *Configuring VLANs, Spanning Tree, and NLB*.	6.0	6.0	6.0	6.0
First Hop Security For more information, see *Configuring Security*.	5.0	5.0	5.0	5.0
IEEE 802.3x Pause frame transmit For more information, see the following documents: • *Administering* • *Monitoring Performance*	6.0	6.0	6.0	6.0
MAC security (MAC-layer filtering, limit learning) For more information, see *Configuring VLANs, Spanning Tree, and NLB*		N/A	N/A	N/A
Media Access Control Security (MACsec) ✳ **Note:** VOSS 5.0 officially removes the replay protection commands. Do not use replay protection in earlier releases.	4.0	4.2.1	4.1	4.2

Table continues…

Features	Release introduced by platform series			
	VSP 4000	**VSP 7200**	**VSP 8200**	**VSP 8400**
For more information, see *Configuring Security*.				
MACsec enhancements For more information, see *Configuring Security*.	6.0	6.0	6.0	6.0
Microsoft Network Load Balancing Service (NLB) — unicast mode For more information, see *Configuring VLANs, Spanning Tree, and NLB*.	N/A	4.2.1	4.0	4.2
Microsoft Network Load Balancing Service (NLB) — multicast mode For more information, see *Configuring VLANs, Spanning Tree, and NLB*.	N/A	6.0	6.0	6.0
MultiLink Trunking (MLT) / Link Aggregation Group (LAG) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST*.	3.0	4.2.1	4.0	4.2
nni-mstp boot flag This flag has special upgrade considerations the first time you upgrade to a release that supports it. For more information, see *Administering*.	6.0	6.0	6.0	6.0
Spanning Tree Protocol (STP) • Multiple Spanning Tree Protocol (MSTP) • Rapid Spanning Tree Protocol (RSTP) For more information, see *Configuring VLANs, Spanning Tree, and NLB*.	3.0	4.2.1	4.0	4.2
VXLAN Gateway For more information, see *Configuring VLANs, Spanning Tree, and NLB*.	N/A	6.0	6.0	6.0
Fabric technologies				
All Fabric Connect services with switch cluster For more information, see *Configuring Fabric Connect*.	4.1	4.2.1	4.0	4.2
ECMP support for VXLAN Gateway and Fabric Extend. For more information, see *Configuring VLANs, Spanning Tree, and NLB*.	N/A	6.0	6.0	6.0
Equal Cost Trees (ECT) For more information, see *Configuring Fabric Connect*.	3.0	4.2.1	4.0	4.2

Table continues…

Features	Release introduced by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
E-Tree and Private VLANs • For more information about E-Tree, see *Configuring Fabric Connect*. • For more information about Private VLANs, see *Configuring VLANs, Spanning Tree, and NLB*. • For information about how to configure MultiLink Trunks (MLT) and Private VLANs, see *Configuring Link Aggregation, MLT, SMLT, and vIST*.	3.0.1	4.2.1	4.1	4.2
Fabric Attach For more information, see *Configuring Fabric Connect*.	5.0	5.0	5.0	5.0
Fabric Attach Zero Touch Client Attachment For more information, see *Configuring Fabric Connect*.	6.0	6.0	6.0	6.0
Fabric Extend For more information, see *Configuring Fabric Connect*.	5.0	5.0	5.0	5.0
Fabric RSPAN (Mirror to I-SID) For more information, see *Troubleshooting*.	6.0	6.0	6.0	6.0
Inter-VSN routing For more information, see *Configuring Fabric Connect*.	3.0	4.2.1	4.0	4.2
IPv6 inter-VSN routing For more information, see *Configuring Fabric Connect*.	4.1	4.2.1	4.1	4.2
IP Multicast over Fabric Connect For more information, see *Configuring Fabric Connect*.	3.1	4.2.1	4.1	4.2
IP Shortcut routing including ECMP For more information, see *Configuring Fabric Connect*.	3.0	4.2.1	4.0	4.2
IPv6 Shortcut routing For more information, see *Configuring Fabric Connect*.	4.1	4.2.1	4.1	4.2
IS-IS accept policies For more information, see *Configuring Fabric Connect*.	4.1	4.2.1	4.1	4.2
Layer 2 Virtual Service Network (VSN) For more information, see *Configuring Fabric Connect*.	3.0	4.2.1	4.0	4.2
Layer 3 VSN For more information, see *Configuring Fabric Connect*.	3.0	4.2.1	4.1	4.2
`run spbm` installation script	4.1	4.2.1	4.1	4.2

Table continues…

Features	Release introduced by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
For more information, see *Configuring Fabric Connect*.				
`run vms endura` script For more information, see *Configuring Fabric Connect*.	4.1	N/A	N/A	N/A
SPB-PIM Gateway controller For more information, see *Configuring SPB-PIM Gateway*.	6.0	6.0	6.0	6.0
SPB-PIM Gateway interface For more information, see *Configuring SPB-PIM Gateway*.	6.0	6.0	6.0	6.0
Switched UNI For more information, see *Configuring Fabric Connect*.	5.0	5.0	5.0	5.0
Transparent Port UNI (T-UNI) For more information, see *Configuring Fabric Connect*.	3.1	4.2.1	4.2.1	4.2.1
Layer 3 IPv4 and IPv6 routing services				
Address Resolution Protocol (ARP) • Proxy ARP • Static ARP For more information, see *Configuring IPv4 Routing*.	3.0	4.2.1	4.0	4.2
Alternative Routes for IPv4 For more information, see *Configuring IPv4 Routing*	3.1	4.2.1	4.0	4.2
Alternative Routes for IPv6 For more information, see *Configuring IPv6 Routing*	5.1	5.1	5.1	5.1
Border Gateway Protocol (BGP) for IPv4 For more information, see *Configuring BGP Services*.	3.1	4.2.1	4.1	4.2
BGP+ (BGP for IPv6) For more information, see *Configuring BGP Services*.	5.0	5.0	5.0	5.0
Internal Border Gateway Protocol (IBGP) For more information, see *Configuring BGP Services*.	4.2	4.2.1	4.2	4.2
External Border Gateway Protocol (EBGP) For more information, see *Configuring BGP Services*.	3.1	4.2.1	4.1	4.2
Distributed Virtual Routing (DvR) controller For more information, see *Configuring IPv4 Routing*	N/A	6.0.1	6.0.1	6.0.1
Distributed Virtual Routing (DvR) leaf For more information, see *Configuring IPv4 Routing*	6.0.1	6.0.1	6.0.1	6.0.1

Table continues…

Features	Release introduced by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
	Demo only			
Dynamic Host Configuration Protocol (DHCP) Relay, DHCP Option 82 For more information, see *Configuring IPv4 Routing*.	3.0	4.2.1	4.0	4.2
DHCP Snooping and Neighbor Discovery Inspection For more information, see *Configuring Security*.	5.1	5.1	5.1	5.1
Equal Cost Multiple Path (ECMP) for IPv4 For more information, see *Configuring IPv4 Routing*.	3.0	4.2.1	4.0	4.2
Equal Cost Multiple Path (ECMP) for IPv6 For more information, see the following documents: • *Configuring IPv4 Routing* • *Configuring IPv6 Routing* • *Configuring BGP Services* • *Configuring Fabric Connect*	5.1	5.1	5.1	5.1
Gratuitous ARP filtering For more information, see *Configuring IPv4 Routing*.	4.2	4.2.1	4.2	4.2
Internet Control Message Protocol (ICMP) For more information, see *Configuring IPv4 Routing*.	3.0	4.2.1	4.0	4.2
Internet Group Management Protocol (IGMP) , including virtualization For more information, see *Configuring IP Multicast Routing Protocols*.	3.0	4.2.1	4.0.1	4.2
IP route policies For more information, see *Configuring IPv4 Routing*.	3.0	4.2.1	4.0	4.2
IPsec for the Out-of-band management port For more information, see *Configuring Security*.	4.2	4.2.1	4.2	4.2
IPv6 (OSPFv3, VRRP, RSMLT, DHCP Relay, IPv4 in IPv6 tunnels) For more information, see *Configuring IPv6 Routing*.	4.1	4.2.1	4.1	4.2
IPv6 mode flag (boot config flags ipv6-mode) For more information, see *Configuring IPv6 Routing*.	N/A			
Layer 3 switch cluster (Routed SMLT) with Virtual Inter-Switch Trunk (vIST)	4.1	4.2.1	4.0	4.2

Table continues…

Features	Release introduced by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST*.				
Layer 3 switch cluster (Routed SMLT) with Simplified vIST For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST*.	4.1	4.2.1	4.0.1	4.2
Multicast Listener Discovery For more information, see *Configuring IP Multicast Routing Protocols*.	5.1	5.1	5.1	5.1
Multicast Route Statistics for IPv4 and IPv6 For more information, see *Configuring IP Multicast Routing Protocols*.	N/A	5.1	5.1	5.1
Open Shortest Path First (OSPF) For more information, see *Configuring OSPF and RIP*.	3.1	4.2.1	4.0	4.2
Protocol Independent Multicast over IPv6 For more information, see *Configuring IP Multicast Routing Protocols*.	5.1	5.1	5.1	5.1
Protocol Independent Multicast–Sparse Mode (PIM-SM), PIM-Source Specific Mode (PIM-SSM) For more information, see *Configuring IP Multicast Routing Protocols*.	4.1	4.2.1	4.0.1	4.2
Route Information Protocol (RIP) For more information, see *Configuring OSPF and RIP*.	3.1	4.2.1	4.0	4.2
RIPng For more information, see *Configuring IPv6 Routing*.	5.0	5.0	5.0	5.0
Static routing For more information, see *Configuring IPv4 Routing*.	3.0	4.2.1	4.0	4.2
Unicast Reverse Path Forwarding (URPF) checking (IPv4 and IPv6) For more information, see *Configuring Security*.	5.0	5.0	5.0	5.0
Virtualization with IPv4 Virtual Routing and Forwarding (VRF) • ARP • DHCP Relay • Inter-VRF Routing (static, dynamic, and policy) • Local Routing • OSPFv2	3.0	4.2.1	4.0	4.2

Table continues…

Features	Release introduced by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
• RIPv1/2 • Route Policies • Static Routing • VRRP For more information, see *Configuring IPv4 Routing*.				
Increased VRF and L3 VSN scaling For more information, see *Configuring IPv4 Routing*.	6.0	6.0	6.0	6.0
Virtual Router Redundancy Protocol (VRRP) • Backup Master For more information, see *Configuring IPv4 Routing*.	3.0	4.2.1	4.0	4.2
VRRPv3 for IPv4 and IPv6 For more information, see the following documents: • *Configuring IPv4 Routing* • *Configuring IPv6 Routing* • *Monitoring Performance*	5.1	5.1	5.1	5.1
Quality of Service and filtering				
Access Control List (ACL)-based filtering • Egress ACLs • Ingress ACLs • Layer 2 to Layer 4 filtering • Port • VLAN For more information, see *Configuring QoS and ACL-Based Traffic Filtering*.	3.0	4.2.1	4.0	4.2
Automatic QoS For more information, see *Configuring QoS and ACL-Based Traffic Filtering*.	3.0	4.2.1	4.0	4.2
Differentiated Services (DiffServ) including Per-Hop Behavior For more information, see *Configuring QoS and ACL-Based Traffic Filtering*.	3.0	4.2.1	4.0	4.2
Egress port shaper For more information, see *Configuring QoS and ACL-Based Traffic Filtering*.	3.0	4.2.1	4.0	4.2

Table continues…

Features	Release introduced by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
Egress port mirror For more information, see *Troubleshooting*	4.0	N/A	N/A	N/A
IPv6 ACL filters For more information, see *Configuring QoS and ACL-Based Traffic Filtering*.	4.1	4.2.1	4.1	4.2
QoS Access Control Entries (ACE) For more information, see *Configuring QoS and ACL-Based Traffic Filtering*.	3.0	4.2.1	4.0	4.2
QoS ingress port rate limiter For more information, see *Configuring QoS and ACL-Based Traffic Filtering*.	n/a	4.2.1	4.0	4.2
QoS per queue rate limiting For more information, see *Configuring QoS and ACL-Based Traffic Filtering*.	5.1	5.1.1	5.1.1	5.1.1
Security ACEs For more information, see *Configuring QoS and ACL-Based Traffic Filtering*.	3.0	4.2.1	4.0	4.2

MIB changes

This section contains information on the MIB changes in this release.

Deprecated MIBs

Object Name	Object OID	Deprecated in Release
msdpRequestsTable	1.3.6.1.3.92.1.1.4	6.0
msdpRequestsEntry	1.3.6.1.3.92.1.1.4.1	6.0
msdpRequestsGroupAddress	1.3.6.1.3.92.1.1.4.1.1	6.0
msdpRequestsGroupMask	1.3.6.1.3.92.1.1.4.1.2	6.0
msdpRequestsPeer	1.3.6.1.3.92.1.1.4.1.3	6.0
msdpRequestsStatus	1.3.6.1.3.92.1.1.4.1.4	6.0
msdpPeerOutSAResponses	1.3.6.1.3.92.1.1.5.1.10	6.0
msdpPeerProcessRequestsFrom	1.3.6.1.3.92.1.1.5.1.24	6.0
msdpPeerInNotifications	1.3.6.1.3.92.1.1.5.1.31	6.0

Table continues…

Object Name	Object OID	Deprecated in Release
msdpPeerOutNotifications	1.3.6.1.3.92.1.1.5.1.32	6.0
msdpPeerLastError	1.3.6.1.3.92.1.1.5.1.33	6.0
msdpPeerInSAResponses	1.3.6.1.3.92.1.1.5.1.9	6.0
msdpMIBPeerGroup	1.3.6.1.3.92.1.1.8.2.2	6.0
msdpMIBRequestsGroup	1.3.6.1.3.92.1.1.8.2.6	6.0
rcIsisLogicalInterfaceNextHopIfIndex	1.3.6.1.4.1.2272.1.63.26.1.11	6.0
rcIsisLogicalInterfaceNextHopVid	1.3.6.1.4.1.2272.1.63.26.1.12	6.0
rcMsdpPeerAsNumber	1.3.6.1.4.1.2272.1.80.1.1.2.1.1	6.0
rcMsdpSACacheTable	1.3.6.1.4.1.2272.1.80.1.1.3	6.0

New MIBs

Object Name	Object OID	Added in Release
msdpMIB	1.3.6.1.3.92	6.0
msdpMIBobjects	1.3.6.1.3.92.1	6.0
msdp	1.3.6.1.3.92.1.1	6.0
msdpTraps	1.3.6.1.3.92.1.1.0	6.0
msdpEstablished	1.3.6.1.3.92.1.1.0.1	6.0
msdpBackwardTransition	1.3.6.1.3.92.1.1.0.2	6.0
msdpEnabled	1.3.6.1.3.92.1.1.1	6.0
msdpRPAddress	1.3.6.1.3.92.1.1.11	6.0
msdpMeshGroupTable	1.3.6.1.3.92.1.1.12	6.0
msdpMeshGroupEntry	1.3.6.1.3.92.1.1.12.1	6.0
msdpMeshGroupName	1.3.6.1.3.92.1.1.12.1.1	6.0
msdpMeshGroupPeerAddress	1.3.6.1.3.92.1.1.12.1.2	6.0
msdpMeshGroupStatus	1.3.6.1.3.92.1.1.12.1.3	6.0
msdpCacheLifetime	1.3.6.1.3.92.1.1.2	6.0
msdpNumSACacheEntries	1.3.6.1.3.92.1.1.3	6.0
msdpPeerTable	1.3.6.1.3.92.1.1.5	6.0
msdpPeerEntry	1.3.6.1.3.92.1.1.5.1	6.0
msdpPeerRemoteAddress	1.3.6.1.3.92.1.1.5.1.1	6.0
msdpPeerOutSAResponses	1.3.6.1.3.92.1.1.5.1.10	6.0
msdpPeerInControlMessages	1.3.6.1.3.92.1.1.5.1.11	6.0

Table continues…

Object Name	Object OID	Added in Release
msdpPeerOutControlMessages	1.3.6.1.3.92.1.1.5.1.12	6.0
msdpPeerInDataPackets	1.3.6.1.3.92.1.1.5.1.13	6.0
msdpPeerOutDataPackets	1.3.6.1.3.92.1.1.5.1.14	6.0
msdpPeerFsmEstablishedTransitions	1.3.6.1.3.92.1.1.5.1.15	6.0
msdpPeerFsmEstablishedTime	1.3.6.1.3.92.1.1.5.1.16	6.0
msdpPeerInMessageTime	1.3.6.1.3.92.1.1.5.1.17	6.0
msdpPeerLocalAddress	1.3.6.1.3.92.1.1.5.1.18	6.0
msdpPeerConnectRetryInterval	1.3.6.1.3.92.1.1.5.1.20	6.0
msdpPeerHoldTimeConfigured	1.3.6.1.3.92.1.1.5.1.21	6.0
msdpPeerKeepAliveConfigured	1.3.6.1.3.92.1.1.5.1.22	6.0
msdpPeerDataTtl	1.3.6.1.3.92.1.1.5.1.23	6.0
msdpPeerProcessRequestsFrom	1.3.6.1.3.92.1.1.5.1.24	6.0
msdpPeerStatus	1.3.6.1.3.92.1.1.5.1.25	6.0
msdpPeerRemotePort	1.3.6.1.3.92.1.1.5.1.26	6.0
msdpPeerLocalPort	1.3.6.1.3.92.1.1.5.1.27	6.0
msdpPeerEncapsulationType	1.3.6.1.3.92.1.1.5.1.29	6.0
msdpPeerState	1.3.6.1.3.92.1.1.5.1.3	6.0
msdpPeerConnectionAttempts	1.3.6.1.3.92.1.1.5.1.30	6.0
msdpPeerInNotifications	1.3.6.1.3.92.1.1.5.1.31	6.0
msdpPeerOutNotifications	1.3.6.1.3.92.1.1.5.1.32	6.0
msdpPeerLastError	1.3.6.1.3.92.1.1.5.1.33	6.0
msdpPeerDiscontinuityTime	1.3.6.1.3.92.1.1.5.1.34	6.0
msdpPeerRPFFailures	1.3.6.1.3.92.1.1.5.1.4	6.0
msdpPeerInSAs	1.3.6.1.3.92.1.1.5.1.5	6.0
msdpPeerOutSAs	1.3.6.1.3.92.1.1.5.1.6	6.0
msdpPeerInSARequests	1.3.6.1.3.92.1.1.5.1.7	6.0
msdpPeerOutSARequests	1.3.6.1.3.92.1.1.5.1.8	6.0
msdpPeerInSAResponses	1.3.6.1.3.92.1.1.5.1.9	6.0
msdpSACacheTable	1.3.6.1.3.92.1.1.6	6.0
msdpSACacheEntry	1.3.6.1.3.92.1.1.6.1	6.0
msdpSACacheGroupAddr	1.3.6.1.3.92.1.1.6.1.1	6.0
msdpSACacheStatus	1.3.6.1.3.92.1.1.6.1.10	6.0
msdpSACacheSourceAddr	1.3.6.1.3.92.1.1.6.1.2	6.0
msdpSACacheOriginRP	1.3.6.1.3.92.1.1.6.1.3	6.0
msdpSACachePeerLearnedFrom	1.3.6.1.3.92.1.1.6.1.4	6.0

Table continues…

Object Name	Object OID	Added in Release
msdpSACacheRPFPeer	1.3.6.1.3.92.1.1.6.1.5	6.0
msdpSACacheInSAs	1.3.6.1.3.92.1.1.6.1.6	6.0
msdpSACacheInDataPackets	1.3.6.1.3.92.1.1.6.1.7	6.0
msdpSACacheUpTime	1.3.6.1.3.92.1.1.6.1.8	6.0
msdpSACacheExpiryTime	1.3.6.1.3.92.1.1.6.1.9	6.0
msdpMIBConformance	1.3.6.1.3.92.1.1.8	6.0
msdpMIBCompliances	1.3.6.1.3.92.1.1.8.1	6.0
msdpMIBCompliance	1.3.6.1.3.92.1.1.8.1.1	6.0
msdpMIBFullCompliance	1.3.6.1.3.92.1.1.8.1.2	6.0
msdpMIBReadOnlyCompliance	1.3.6.1.3.92.1.1.8.1.3	6.0
msdpMIBGroups	1.3.6.1.3.92.1.1.8.2	6.0
msdpMIBGlobalsGroup	1.3.6.1.3.92.1.1.8.2.1	6.0
msdpMIBEncapsulationGroup	1.3.6.1.3.92.1.1.8.2.3	6.0
msdpMIBSACacheGroup	1.3.6.1.3.92.1.1.8.2.4	6.0
msdpMIBNotificationGroup	1.3.6.1.3.92.1.1.8.2.5	6.0
msdpMIBRPGroup	1.3.6.1.3.92.1.1.8.2.7	6.0
msdpMIBMeshGroupGroup	1.3.6.1.3.92.1.1.8.2.8	6.0
msdpMIBPeerGroup2	1.3.6.1.3.92.1.1.8.2.9	6.0
sflow	1.3.6.1.4.1.14706	6.0
sFlowMIB	1.3.6.1.4.1.14706.1	6.0
sFlowAgent	1.3.6.1.4.1.14706.1.1	6.0
sFlowRcvrTable	1.3.6.1.4.1.14706.1.1.4	6.0
sFlowRcvrEntry	1.3.6.1.4.1.14706.1.1.4.1	6.0
sFlowRcvrIndex	1.3.6.1.4.1.14706.1.1.4.1.1	6.0
sFlowRcvrOwner	1.3.6.1.4.1.14706.1.1.4.1.2	6.0
sFlowRcvrTimeout	1.3.6.1.4.1.14706.1.1.4.1.3	6.0
sFlowRcvrMaximumDatagramSize	1.3.6.1.4.1.14706.1.1.4.1.4	6.0
sFlowRcvrAddressType	1.3.6.1.4.1.14706.1.1.4.1.5	6.0
sFlowRcvrAddress	1.3.6.1.4.1.14706.1.1.4.1.6	6.0
sFlowRcvrPort	1.3.6.1.4.1.14706.1.1.4.1.7	6.0

Table continues…

Object Name	Object OID	Added in Release
sFlowRcvrDatagramVersion	1.3.6.1.4.1.14706.1.1.4.1.8	6.0
sFlowFsTable	1.3.6.1.4.1.14706.1.1.5	6.0
sFlowFsEntry	1.3.6.1.4.1.14706.1.1.5.1	6.0
sFlowFsDataSource	1.3.6.1.4.1.14706.1.1.5.1.1	6.0
sFlowFsInstance	1.3.6.1.4.1.14706.1.1.5.1.2	6.0
sFlowFsReceiver	1.3.6.1.4.1.14706.1.1.5.1.3	6.0
sFlowFsPacketSamplingRate	1.3.6.1.4.1.14706.1.1.5.1.4	6.0
sFlowFsMaximumHeaderSize	1.3.6.1.4.1.14706.1.1.5.1.5	6.0
sFlowCpTable	1.3.6.1.4.1.14706.1.1.6	6.0
sFlowCpEntry	1.3.6.1.4.1.14706.1.1.6.1	6.0
sFlowCpDataSource	1.3.6.1.4.1.14706.1.1.6.1.1	6.0
sFlowCpInstance	1.3.6.1.4.1.14706.1.1.6.1.2	6.0
sFlowCpReceiver	1.3.6.1.4.1.14706.1.1.6.1.3	6.0
sFlowCpInterval	1.3.6.1.4.1.14706.1.1.6.1.4	6.0
rc2kBootConfigEnableVxlanGwFullInterworkingMode	1.3.6.1.4.1.2272.1.100.5.1.52	6.0
rc2kBootConfigEnableDvrLeafMode	1.3.6.1.4.1.2272.1.100.5.1.54	6.0
rcBridgeVnidFdbTable	1.3.6.1.4.1.2272.1.14.24	6.0
rcBridgeVnidFdbEntry	1.3.6.1.4.1.2272.1.14.24.1	6.0
rcBridgeVnidFdbVnid	1.3.6.1.4.1.2272.1.14.24.1.1	6.0
rcBridgeVnidFdbAddress	1.3.6.1.4.1.2272.1.14.24.1.2	6.0
rcBridgeVnidFdbStatus	1.3.6.1.4.1.2272.1.14.24.1.3	6.0
rcBridgeVnidFdbInterfaceIndex	1.3.6.1.4.1.2272.1.14.24.1.4	6.0

Table continues…

Object Name	Object OID	Added in Release
rcBridgeVnidFdbType	1.3.6.1.4.1.2272.1.14.24.1.5	6.0
rcPrFilterAceMonitoringIsidOffset	1.3.6.1.4.1.2272.1.202.1.1.2.4.1.1.32	6.0
rcPrFilterAceMonitoringIsid	1.3.6.1.4.1.2272.1.202.1.1.2.4.1.1.33	6.0
rcPrFilterAceMirroringQos	1.3.6.1.4.1.2272.1.202.1.1.2.4.1.1.34	6.0
rcPrFilterAceRemoveTag	1.3.6.1.4.1.2272.1.202.1.1.2.4.1.1.35	6.0
rcPrFilterAceProtoShowIcmpv6MsgTypeList	1.3.6.1.4.1.2272.1.202.1.1.2.4.27.1.24	6.0
rcPrFilterAceProtoShowIcmpv6MsgTypeOper	1.3.6.1.4.1.2272.1.202.1.1.2.4.27.1.25	6.0
rcPrFilterAceProtoIcmpv6MsgTypeTable	1.3.6.1.4.1.2272.1.202.1.1.2.4.38.1	6.0
rcVxlan	1.3.6.1.4.1.2272.1.218	6.0
rcVxlanVtepSourceIp	1.3.6.1.4.1.2272.1.218.1	6.0
rcVxlanVtepVrf	1.3.6.1.4.1.2272.1.218.2	6.0
rcVxlanVtepTable	1.3.6.1.4.1.2272.1.218.3	6.0
rcVxlanVtepEntry	1.3.6.1.4.1.2272.1.218.3.1	6.0
rcVxlanVtepId	1.3.6.1.4.1.2272.1.218.3.1.1	6.0
rcVxlanVtepIpAddr	1.3.6.1.4.1.2272.1.218.3.1.2	6.0
rcVxlanVtepName	1.3.6.1.4.1.2272.1.218.3.1.3	6.0
rcVxlanVtepRowStatus	1.3.6.1.4.1.2272.1.218.3.1.4	6.0
rcVxlanVtepNextHopVrfName	1.3.6.1.4.1.2272.1.218.3.1.5	6.0
rcVxlanVnidTable	1.3.6.1.4.1.2272.1.218.4	6.0
rcVxlanVnidEntry	1.3.6.1.4.1.2272.1.218.4.1	6.0
rcVxlanVnidIdentifier	1.3.6.1.4.1.2272.1.218.4.1.1	6.0
rcVxlanVnidIsid	1.3.6.1.4.1.2272.1.218.4.1.2	6.0

Table continues…

Object Name	Object OID	Added in Release
rcVxlanVnidRowStatus	1.3.6.1.4.1.2272.1.218.4.1.3	6.0
rcVxlanVnidAction	1.3.6.1.4.1.2272.1.218.4.1.4	6.0
rcVxlanVnidEndPointTable	1.3.6.1.4.1.2272.1.218.5	6.0
rcVxlanVnidEndPointEntry	1.3.6.1.4.1.2272.1.218.5.1	6.0
rcVxlanVnidEndPointVnid	1.3.6.1.4.1.2272.1.218.5.1.1	6.0
rcVxlanVnidEndPointVtepId	1.3.6.1.4.1.2272.1.218.5.1.2	6.0
rcVxlanVnidEndPointIsid	1.3.6.1.4.1.2272.1.218.5.1.3	6.0
rcVxlanVnidEndPointRowStatus	1.3.6.1.4.1.2272.1.218.5.1.4	6.0
rcVxlanVtepNextHopTable	1.3.6.1.4.1.2272.1.218.6	6.0
rcVxlanVtepNextHopEntry	1.3.6.1.4.1.2272.1.218.6.1	6.0
rcVxlanVtepNextHopVtepId	1.3.6.1.4.1.2272.1.218.6.1.1	6.0
rcVxlanVtepNextHopIp	1.3.6.1.4.1.2272.1.218.6.1.2	6.0
rcVxlanVtepNextHopIfIndex	1.3.6.1.4.1.2272.1.218.6.1.3	6.0
rcVxlanVtepNextHopVid	1.3.6.1.4.1.2272.1.218.6.1.4	6.0
rcVxlanVnidElanEndPointTable	1.3.6.1.4.1.2272.1.218.7	6.0
rcVxlanVnidElanEndPointEntry	1.3.6.1.4.1.2272.1.218.7.1	6.0
rcVxlanVnidElanEndPointVnid	1.3.6.1.4.1.2272.1.218.7.1.1	6.0
rcVxlanVnidElanEndPointCvid	1.3.6.1.4.1.2272.1.218.7.1.2	6.0
rcVxlanVnidElanEndPointIfIndex	1.3.6.1.4.1.2272.1.218.7.1.3	6.0
rcVxlanVnidElanEndPointIsid	1.3.6.1.4.1.2272.1.218.7.1.4	6.0
rcVxlanVnidElanEndPointRowStatus	1.3.6.1.4.1.2272.1.218.7.1.5	6.0
rcDvr	1.3.6.1.4.1.2272.1.219	6.0

Table continues…

Object Name	Object OID	Added in Release
rcDvrGlobal	1.3.6.1.4.1.2272.1.219.1	6.0
rcDvrGlobalDomainId	1.3.6.1.4.1.2272.1.219.1.1	6.0
rcDvrGlobalGatewayMac	1.3.6.1.4.1.2272.1.219.1.10	6.0
rcDvrGlobalInbandMgmtIp	1.3.6.1.4.1.2272.1.219.1.11	6.0
rcDvrGlobalInjectDefaultRouteDisable	1.3.6.1.4.1.2272.1.219.1.12	6.0
rcDvrGlobalOperState	1.3.6.1.4.1.2272.1.219.1.13	6.0
rcDvrGlobalSystemIdAsMac	1.3.6.1.4.1.2272.1.219.1.14	6.0
rcDvrGlobalRole	1.3.6.1.4.1.2272.1.219.1.2	6.0
rcDvrGlobalEnable	1.3.6.1.4.1.2272.1.219.1.3	6.0
rcDvrVirtualIstLocalAddr	1.3.6.1.4.1.2272.1.219.1.4	6.0
rcDvrVirtualIstLocalMask	1.3.6.1.4.1.2272.1.219.1.5	6.0
rcDvrVirtualIstPeerAddr	1.3.6.1.4.1.2272.1.219.1.6	6.0
rcDvrVirtualIstClusterId	1.3.6.1.4.1.2272.1.219.1.7	6.0
rcDvrGlobalDomainIsid	1.3.6.1.4.1.2272.1.219.1.8	6.0
rcDvrGlobalBackboneIsid	1.3.6.1.4.1.2272.1.219.1.9	6.0
rcDvrRouteTable	1.3.6.1.4.1.2272.1.219.2	6.0
rcDvrRouteEntry	1.3.6.1.4.1.2272.1.219.2.1	6.0
rcDvrRouteDestIpAddrType	1.3.6.1.4.1.2272.1.219.2.1.1	6.0
rcDvrRouteType	1.3.6.1.4.1.2272.1.219.2.1.10	6.0
rcDvrRouteDestIpAddr	1.3.6.1.4.1.2272.1.219.2.1.2	6.0
rcDvrRouteDestMask	1.3.6.1.4.1.2272.1.219.2.1.3	6.0

Table continues…

Object Name	Object OID	Added in Release
rcDvrRouteL3Isid	1.3.6.1.4.1.2272.1.219.2.1.4	6.0
rcDvrRouteEcmpIndex	1.3.6.1.4.1.2272.1.219.2.1.5	6.0
rcDvrRouteNextHopMac	1.3.6.1.4.1.2272.1.219.2.1.6	6.0
rcDvrRouteL2Isid	1.3.6.1.4.1.2272.1.219.2.1.7	6.0
rcDvrRouteCost	1.3.6.1.4.1.2272.1.219.2.1.8	6.0
rcDvrRouteNextHopName	1.3.6.1.4.1.2272.1.219.2.1.9	6.0
rcDvrMembersTable	1.3.6.1.4.1.2272.1.219.3	6.0
rcDvrMembersEntry	1.3.6.1.4.1.2272.1.219.3.1	6.0
rcDvrMemberMacAddress	1.3.6.1.4.1.2272.1.219.3.1.1	6.0
rcDvrMemberSysId	1.3.6.1.4.1.2272.1.219.3.1.2	6.0
rcDvrMemberNickName	1.3.6.1.4.1.2272.1.219.3.1.3	6.0
rcDvrMemberRole	1.3.6.1.4.1.2272.1.219.3.1.4	6.0
rcDvrMemberDomainId	1.3.6.1.4.1.2272.1.219.3.1.5	6.0
rcDvrInterfacesTable	1.3.6.1.4.1.2272.1.219.4	6.0
rcDvrInterfacesEntry	1.3.6.1.4.1.2272.1.219.4.1	6.0
rcDvrInterfaceVlanIpAddrType	1.3.6.1.4.1.2272.1.219.4.1.1	6.0
rcDvrInterfaceAdminState	1.3.6.1.4.1.2272.1.219.4.1.10	6.0
rcDvrInterfaceSpbmcState	1.3.6.1.4.1.2272.1.219.4.1.11	6.0
rcDvrInterfaceIgmpVersion	1.3.6.1.4.1.2272.1.219.4.1.12	6.0
rcDvrInterfaceVlanIpAddr	1.3.6.1.4.1.2272.1.219.4.1.2	6.0
rcDvrInterfaceL3Isid	1.3.6.1.4.1.2272.1.219.4.1.3	6.0

Table continues…

Object Name	Object OID	Added in Release
rcDvrInterfaceL2Isid	1.3.6.1.4.1.2272.1.219.4.1.4	6.0
rcDvrInterfaceVlanIpMask	1.3.6.1.4.1.2272.1.219.4.1.5	6.0
rcDvrInterfaceVrfId	1.3.6.1.4.1.2272.1.219.4.1.6	6.0
rcDvrInterfaceVlanId	1.3.6.1.4.1.2272.1.219.4.1.7	6.0
rcDvrInterfaceGwIpAddrType	1.3.6.1.4.1.2272.1.219.4.1.8	6.0
rcDvrInterfaceGwIpAddr	1.3.6.1.4.1.2272.1.219.4.1.9	6.0
rcDvrHostEntriesTable	1.3.6.1.4.1.2272.1.219.5	6.0
rcDvrHostEntriesEntry	1.3.6.1.4.1.2272.1.219.5.1	6.0
rcDvrHostEntriesIpAddrType	1.3.6.1.4.1.2272.1.219.5.1.1	6.0
rcDvrHostEntriesNextHopName	1.3.6.1.4.1.2272.1.219.5.1.10	6.0
rcDvrHostEntriesNextHopMac	1.3.6.1.4.1.2272.1.219.5.1.11	6.0
rcDvrHostEntriesIpAddr	1.3.6.1.4.1.2272.1.219.5.1.2	6.0
rcDvrHostEntriesMask	1.3.6.1.4.1.2272.1.219.5.1.3	6.0
rcDvrHostEntriesL3Isid	1.3.6.1.4.1.2272.1.219.5.1.4	6.0
rcDvrHostEntriesMacAddr	1.3.6.1.4.1.2272.1.219.5.1.5	6.0
rcDvrHostEntriesL2Isid	1.3.6.1.4.1.2272.1.219.5.1.6	6.0
rcDvrHostEntriesPort	1.3.6.1.4.1.2272.1.219.5.1.7	6.0
rcDvrHostEntriesDomainId	1.3.6.1.4.1.2272.1.219.5.1.8	6.0
rcDvrHostEntriesType	1.3.6.1.4.1.2272.1.219.5.1.9	6.0
rcDvrL3vsnTable	1.3.6.1.4.1.2272.1.219.6	6.0
rcDvrL3vsnEntry	1.3.6.1.4.1.2272.1.219.6.1	6.0

Table continues…

Object Name	Object OID	Added in Release
rcDvrL3vsnVrfId	1.3.6.1.4.1.2272.1.219.6.1.1	6.0
rcDvrL3vsnIsid	1.3.6.1.4.1.2272.1.219.6.1.2	6.0
rcDvrL3vsnVrfName	1.3.6.1.4.1.2272.1.219.6.1.3	6.0
rcDvrDatabaseTable	1.3.6.1.4.1.2272.1.219.7	6.0
rcDvrDatabaseEntry	1.3.6.1.4.1.2272.1.219.7.1	6.0
rcDvrDatabaseDestIpAddrType	1.3.6.1.4.1.2272.1.219.7.1.1	6.0
rcDvrDatabasePrefixCost	1.3.6.1.4.1.2272.1.219.7.1.10	6.0
rcDvrDatabaseNextHopName	1.3.6.1.4.1.2272.1.219.7.1.11	6.0
rcDvrDatabaseAge	1.3.6.1.4.1.2272.1.219.7.1.12	6.0
rcDvrDatabaseDestIpAddr	1.3.6.1.4.1.2272.1.219.7.1.2	6.0
rcDvrDatabaseDestMask	1.3.6.1.4.1.2272.1.219.7.1.3	6.0
rcDvrDatabaseL3Isid	1.3.6.1.4.1.2272.1.219.7.1.4	6.0
rcDvrDatabaseEcmpIndex	1.3.6.1.4.1.2272.1.219.7.1.5	6.0
rcDvrDatabaseNextHop	1.3.6.1.4.1.2272.1.219.7.1.6	6.0
rcDvrDatabaseL2Isid	1.3.6.1.4.1.2272.1.219.7.1.7	6.0
rcDvrDatabaseOutgoingInterface	1.3.6.1.4.1.2272.1.219.7.1.8	6.0
rcDvrDatabaseSpbCost	1.3.6.1.4.1.2272.1.219.7.1.9	6.0
rcDvrBackboneEntriesTable	1.3.6.1.4.1.2272.1.219.8	6.0
rcDvrBackboneEntriesEntry	1.3.6.1.4.1.2272.1.219.8.1	6.0
rcDvrBackboneEntriesIpAddrType	1.3.6.1.4.1.2272.1.219.8.1.1	6.0
rcDvrBackboneEntriesNextHopName	1.3.6.1.4.1.2272.1.219.8.1.10	6.0

Table continues…

Object Name	Object OID	Added in Release
rcDvrBackboneEntriesNextHopMac	1.3.6.1.4.1.2272.1.219.8.1.11	6.0
rcDvrBackboneEntriesIpAddr	1.3.6.1.4.1.2272.1.219.8.1.2	6.0
rcDvrBackboneEntriesL3Isid	1.3.6.1.4.1.2272.1.219.8.1.3	6.0
rcDvrBackboneEntriesDomainId	1.3.6.1.4.1.2272.1.219.8.1.4	6.0
rcDvrBackboneEntriesEcmpIndex	1.3.6.1.4.1.2272.1.219.8.1.5	6.0
rcDvrBackboneEntriesHostMacAddr	1.3.6.1.4.1.2272.1.219.8.1.6	6.0
rcDvrBackboneEntriesL2Isid	1.3.6.1.4.1.2272.1.219.8.1.7	6.0
rcDvrBackboneEntriesAdvControllerName	1.3.6.1.4.1.2272.1.219.8.1.8	6.0
rcDvrBackboneEntriesAdvController	1.3.6.1.4.1.2272.1.219.8.1.9	6.0
rcDvrBackboneMembersTable	1.3.6.1.4.1.2272.1.219.9	6.0
rcDvrBackboneMembersEntry	1.3.6.1.4.1.2272.1.219.9.1	6.0
rcDvrBackboneMemberMacAddress	1.3.6.1.4.1.2272.1.219.9.1.1	6.0
rcDvrBackboneMemberSysId	1.3.6.1.4.1.2272.1.219.9.1.2	6.0
rcDvrBackboneMemberNickName	1.3.6.1.4.1.2272.1.219.9.1.3	6.0
rcDvrBackboneMemberRole	1.3.6.1.4.1.2272.1.219.9.1.4	6.0
rcDvrBackboneMemberDomainId	1.3.6.1.4.1.2272.1.219.9.1.5	6.0
rcSflow	1.3.6.1.4.1.2272.1.221	6.0
rcSflowMib	1.3.6.1.4.1.2272.1.221.1	6.0
rcSflowObjects	1.3.6.1.4.1.2272.1.221.1.1	6.0
rcSflowScalars	1.3.6.1.4.1.2272.1.221.1.1.1	6.0
rcSflowAdminEnable	1.3.6.1.4.1.2272.1.221.1.1.1.1	6.0

Table continues…

Object Name	Object OID	Added in Release
rcSflowAgentAddressType	1.3.6.1.4.1.2272.1.221.1.1.1.2	6.0
rcSflowAgentAddress	1.3.6.1.4.1.2272.1.221.1.1.1.3	6.0
rcSflowStatsTable	1.3.6.1.4.1.2272.1.221.1.1.2	6.0
rcSflowStatsEntry	1.3.6.1.4.1.2272.1.221.1.1.2.1	6.0
rcSflowStatsIndex	1.3.6.1.4.1.2272.1.221.1.1.2.1.1	6.0
rcSflowStatsDatagramCount	1.3.6.1.4.1.2272.1.221.1.1.2.1.2	6.0
rcSflowStatsClearStats	1.3.6.1.4.1.2272.1.221.1.1.2.1.3	6.0
rcDiagMirrorMonitoringIsidOffset	1.3.6.1.4.1.2272.1.23.1.1.21	6.0
rcDiagMirrorMonitoringIsid	1.3.6.1.4.1.2272.1.23.1.1.22	6.0
rcDiagMirrorMirroringQos	1.3.6.1.4.1.2272.1.23.1.1.23	6.0
rcDiagMonitorByIsidTable	1.3.6.1.4.1.2272.1.23.18	6.0
rcDiagMonitorByIsidEntry	1.3.6.1.4.1.2272.1.23.18.1	6.0
rcDiagMonitorByIsidIndex	1.3.6.1.4.1.2272.1.23.18.1.1	6.0
rcDiagMonitorByIsidMonitorIsidOffset	1.3.6.1.4.1.2272.1.23.18.1.2	6.0
rcDiagMonitorByIsidMonitorIsid	1.3.6.1.4.1.2272.1.23.18.1.3	6.0
rcDiagMonitorByIsidEgressPortList	1.3.6.1.4.1.2272.1.23.18.1.4	6.0
rcDiagMonitorByIsidEgressMltId	1.3.6.1.4.1.2272.1.23.18.1.5	6.0
rcDiagMonitorByIsidMapToVlanId	1.3.6.1.4.1.2272.1.23.18.1.6	6.0
rcDiagMonitorByIsidEnable	1.3.6.1.4.1.2272.1.23.18.1.8	6.0
rcDiagMonitorByIsidRowStatus	1.3.6.1.4.1.2272.1.23.18.1.9	6.0
rcDiagIsidMirroringStatsTable	1.3.6.1.4.1.2272.1.23.19	6.0

Table continues…

Object Name	Object OID	Added in Release
rcDiagIsidMirroringStatsEntry	1.3.6.1.4.1.2272.1.23.19.1	6.0
rcDiagIsidMirroringStatsIndex	1.3.6.1.4.1.2272.1.23.19.1.1	6.0
rcDiagIsidMirroringStatsMonitorIsid	1.3.6.1.4.1.2272.1.23.19.1.2	6.0
rcDiagIsidMirroringStatsMirroredPackets	1.3.6.1.4.1.2272.1.23.19.1.3	6.0
rcDiagIsidMirroringStatsClearStats	1.3.6.1.4.1.2272.1.23.19.1.4	6.0
rcVlanPimGatewayEnable	1.3.6.1.4.1.2272.1.3.2.1.73	6.0
rcVlanDvrEnable	1.3.6.1.4.1.2272.1.3.2.1.76	6.0
rcVlanDvrGwIpv4Addr	1.3.6.1.4.1.2272.1.3.2.1.77	6.0
rcPortBpduGuardTimerCount	1.3.6.1.4.1.2272.1.4.10.1.1.117	6.0
rcIsisGlobalBackboneEnable	1.3.6.1.4.1.2272.1.63.1.22	6.0
rcIsisLogicalInterfaceNextHopTable	1.3.6.1.4.1.2272.1.63.28	6.0
rcIsisLogicalInterfaceNextHopEntry	1.3.6.1.4.1.2272.1.63.28.1	6.0
rcIsisLogicalInterfaceNextHopId	1.3.6.1.4.1.2272.1.63.28.1.1	6.0
rcIsisLogicalInterfaceNextHopIp	1.3.6.1.4.1.2272.1.63.28.1.2	6.0
rcIsisLogicalInterfaceNextHopDestIfIndex	1.3.6.1.4.1.2272.1.63.28.1.3	6.0
rcIsisLogicalInterfaceNextHopDestVid	1.3.6.1.4.1.2272.1.63.28.1.4	6.0
rcIsisPlsbMcastSpbPimGwControllerEnable	1.3.6.1.4.1.2272.1.63.4.1.15	6.0
rcIsisPlsbMcastSpbPimGwGatewayEnable	1.3.6.1.4.1.2272.1.63.4.1.16	6.0
rcIpConfPimGatewayEnable	1.3.6.1.4.1.2272.1.8.1.1.1.30	6.0
rcIpSpbPimGw	1.3.6.1.4.1.2272.1.8.114	6.0
rcIpSpbPimGwGlobal	1.3.6.1.4.1.2272.1.8.114.1	6.0

Table continues…

Object Name	Object OID	Added in Release
rcIpSpbPimGwGlobalHelloInterval	1.3.6.1.4.1.2272.1.8.114.1.1	6.0
rcIpSpbPimGwGlobalJoinPruneInterval	1.3.6.1.4.1.2272.1.8.114.1.2	6.0
rcIpSpbPimGwInterfaceTable	1.3.6.1.4.1.2272.1.8.114.2	6.0
rcIpSpbPimGwInterfaceEntry	1.3.6.1.4.1.2272.1.8.114.2.1	6.0
rcIpSpbPimGwInterfaceIfIndex	1.3.6.1.4.1.2272.1.8.114.2.1.1	6.0
rcIpSpbPimGwInterfaceOperState	1.3.6.1.4.1.2272.1.8.114.2.1.2	6.0
rcIpSpbPimGwInterfaceAddressType	1.3.6.1.4.1.2272.1.8.114.2.1.3	6.0
rcIpSpbPimGwInterfaceAddress	1.3.6.1.4.1.2272.1.8.114.2.1.4	6.0
rcIpSpbPimGwInterfaceAddressMask	1.3.6.1.4.1.2272.1.8.114.2.1.5	6.0
rcIpSpbPimGwInterfaceHelloInterval	1.3.6.1.4.1.2272.1.8.114.2.1.6	6.0
rcIpSpbPimGwInterfaceJoinPruneInterval	1.3.6.1.4.1.2272.1.8.114.2.1.7	6.0
rcIpSpbPimGwNeighborTable	1.3.6.1.4.1.2272.1.8.114.3	6.0
rcIpSpbPimGwNeighborEntry	1.3.6.1.4.1.2272.1.8.114.3.1	6.0
rcIpSpbPimGwNeighborIfIndex	1.3.6.1.4.1.2272.1.8.114.3.1.1	6.0
rcIpSpbPimGwNeighborAddressType	1.3.6.1.4.1.2272.1.8.114.3.1.2	6.0
rcIpSpbPimGwNeighborAddress	1.3.6.1.4.1.2272.1.8.114.3.1.3	6.0
rcIpSpbPimGwNeighborUpTime	1.3.6.1.4.1.2272.1.8.114.3.1.4	6.0
rcIpSpbPimGwNeighborExpiryTime	1.3.6.1.4.1.2272.1.8.114.3.1.5	6.0
rcIpSpbPimGwControllerForeignSrcTable	1.3.6.1.4.1.2272.1.8.114.4	6.0
rcIpSpbPimGwControllerForeignSrcEntry	1.3.6.1.4.1.2272.1.8.114.4.1	6.0
rcIpSpbPimGwControllerForeignSrcSourceAddress	1.3.6.1.4.1.2272.1.8.114.4.1.1	6.0

Table continues…

Object Name	Object OID	Added in Release
rcIpSpbPimGwControllerForeignSrcGroupAddress	1.3.6.1.4.1.2272.1.8.114.4.1.2	6.0
rcIpSpbPimGwControllerForeignSrcRowStatus	1.3.6.1.4.1.2272.1.8.114.4.1.3	6.0
rcIpSpbPimGwControllerForeignSrcGatewaySysId	1.3.6.1.4.1.2272.1.8.114.4.1.4	6.0
rcIpSpbPimGwControllerForeignSrcGatewayHostName	1.3.6.1.4.1.2272.1.8.114.4.1.5	6.0
rcIpSpbPimGwControllerForeignSrcType	1.3.6.1.4.1.2272.1.8.114.4.1.6	6.0
rcIpSpbPimGwControllerForeignSrcOwner	1.3.6.1.4.1.2272.1.8.114.4.1.7	6.0
rcIpSpbPimGwControllerSpbmcSrcTable	1.3.6.1.4.1.2272.1.8.114.5	6.0
rcIpSpbPimGwControllerSpbmcSrcEntry	1.3.6.1.4.1.2272.1.8.114.5.1	6.0
rcIpSpbPimGwControllerSpbmcSrcSourceAddress	1.3.6.1.4.1.2272.1.8.114.5.1.1	6.0
rcIpSpbPimGwControllerSpbmcSrcGroupAddress	1.3.6.1.4.1.2272.1.8.114.5.1.2	6.0
rcIpSpbPimGwControllerSpbmcSrcOriginatorSysId	1.3.6.1.4.1.2272.1.8.114.5.1.3	6.0
rcIpSpbPimGwControllerSpbmcSrcOriginatorHostName	1.3.6.1.4.1.2272.1.8.114.5.1.4	6.0
rcIpSpbPimGwGatewayForeignSrcTable	1.3.6.1.4.1.2272.1.8.114.6	6.0
rcIpSpbPimGwGatewayForeignSrcEntry	1.3.6.1.4.1.2272.1.8.114.6.1	6.0
rcIpSpbPimGwGatewayForeignSrcSourceAddress	1.3.6.1.4.1.2272.1.8.114.6.1.1	6.0
rcIpSpbPimGwGatewayForeignSrcGroupAddress	1.3.6.1.4.1.2272.1.8.114.6.1.2	6.0
rcIpSpbPimGwGatewayForeignSrcControllerSysId	1.3.6.1.4.1.2272.1.8.114.6.1.3	6.0
rcIpSpbPimGwGatewayForeignSrcControllerHostName	1.3.6.1.4.1.2272.1.8.114.6.1.4	6.0
rcIpSpbPimGwGatewayForeignSrcGatewaySysId	1.3.6.1.4.1.2272.1.8.114.6.1.5	6.0
rcIpSpbPimGwGatewayForeignSrcGatewayHostName	1.3.6.1.4.1.2272.1.8.114.6.1.6	6.0
rcIpSpbPimGwGatewayForeignSrcInVid	1.3.6.1.4.1.2272.1.8.114.6.1.7	6.0

Table continues…

Object Name	Object OID	Added in Release
rcIpSpbPimGwGatewayForeignSrcInPort	1.3.6.1.4.1.2272.1.8.114.6.1.8	6.0
rcIpSpbPimGwGatewayForeignSrcOwnerType	1.3.6.1.4.1.2272.1.8.114.6.1.9	6.0
rcMRouteExt	1.3.6.1.4.1.2272.1.8.115	6.0
rcMRouteExtTable	1.3.6.1.4.1.2272.1.8.115.1	6.0
rcMRouteExtEntry	1.3.6.1.4.1.2272.1.8.115.1.1	6.0
rcMRouteExtProtocol	1.3.6.1.4.1.2272.1.8.115.1.1.1	6.0
rcMRouteExtNextHopTable	1.3.6.1.4.1.2272.1.8.115.2	6.0
rcMRouteExtNextHopEntry	1.3.6.1.4.1.2272.1.8.115.2.1	6.0
rcMRouteExtNextHopProtocol	1.3.6.1.4.1.2272.1.8.115.2.1.1	6.0
rcMRouteExtNextHopL2Isid	1.3.6.1.4.1.2272.1.8.115.2.1.2	6.0
rcMRouteExtInterfaceTable	1.3.6.1.4.1.2272.1.8.115.3	6.0
rcMRouteExtInterfaceEntry	1.3.6.1.4.1.2272.1.8.115.3.1	6.0
rcMRouteExtInterfaceProtocol	1.3.6.1.4.1.2272.1.8.115.3.1.1	6.0
rcMsdp	1.3.6.1.4.1.2272.1.80	6.0
rcMsdpMib	1.3.6.1.4.1.2272.1.80.1	6.0
rcMsdpObjects	1.3.6.1.4.1.2272.1.80.1.1	6.0
rcMsdpScalars	1.3.6.1.4.1.2272.1.80.1.1.1	6.0
rcMsdpRouteMapName	1.3.6.1.4.1.2272.1.80.1.1.1.1	6.0
rcMsdpRedistributeFilterEnabled	1.3.6.1.4.1.2272.1.80.1.1.1.2	6.0
rcMsdpRedistributeFilterApply	1.3.6.1.4.1.2272.1.80.1.1.1.3	6.0
rcMsdpImplicitDefaultPeerEnabled	1.3.6.1.4.1.2272.1.80.1.1.1.4	6.0
rcMsdpSACacheClear	1.3.6.1.4.1.2272.1.80.1.1.1.6	6.0
rcMsdpStatsClear	1.3.6.1.4.1.2272.1.80.1.1.1.7	6.0

Table continues…

Object Name	Object OID	Added in Release
rcMsdpPeerTable	1.3.6.1.4.1.2272.1.80.1.1.2	6.0
rcMsdpPeerEntry	1.3.6.1.4.1.2272.1.80.1.1.2.1	6.0
rcMsdpPeerAsNumber	1.3.6.1.4.1.2272.1.80.1.1.2.1.1	6.0
rcMsdpPeerDescription	1.3.6.1.4.1.2272.1.80.1.1.2.1.10	6.0
rcMsdpPeerSALimit	1.3.6.1.4.1.2272.1.80.1.1.2.1.11	6.0
rcMsdpPeerMd5AuthEnabled	1.3.6.1.4.1.2272.1.80.1.1.2.1.12	6.0
rcMsdpPeerMd5AuthPassword	1.3.6.1.4.1.2272.1.80.1.1.2.1.13	6.0
rcMsdpPeerSAsLearnedFromThisPeer	1.3.6.1.4.1.2272.1.80.1.1.2.1.14	6.0
rcMsdpPeerSAsAdvertisedToThisPeer	1.3.6.1.4.1.2272.1.80.1.1.2.1.15	6.0
rcMsdpPeerUpOrDownTime	1.3.6.1.4.1.2272.1.80.1.1.2.1.16	6.0
rcMsdpPeerConnAndStatsClearedTime	1.3.6.1.4.1.2272.1.80.1.1.2.1.17	6.0
rcMsdpPeerRouteMapName	1.3.6.1.4.1.2272.1.80.1.1.2.1.18	6.0
rcMsdpPeerAdminEnabled	1.3.6.1.4.1.2272.1.80.1.1.2.1.19	6.0
rcMsdpPeerTooShortMessages	1.3.6.1.4.1.2272.1.80.1.1.2.1.2	6.0
rcMsdpPeerOperEnabled	1.3.6.1.4.1.2272.1.80.1.1.2.1.20	6.0
rcMsdpPeerClearPeer	1.3.6.1.4.1.2272.1.80.1.1.2.1.23	6.0
rcMsdpPeer4ByteAsNumber	1.3.6.1.4.1.2272.1.80.1.1.2.1.24	6.0
rcMsdpPeerInBadMessages	1.3.6.1.4.1.2272.1.80.1.1.2.1.3	6.0
rcMsdpPeerInKeepAliveMessages	1.3.6.1.4.1.2272.1.80.1.1.2.1.4	6.0
rcMsdpPeerOutKeepAliveMessages	1.3.6.1.4.1.2272.1.80.1.1.2.1.5	6.0

Table continues…

Object Name	Object OID	Added in Release
rcMsdpPeerInSAFilterEnabled	1.3.6.1.4.1.2272.1.80.1.1.2.1.6	6.0
rcMsdpPeerInSAFilterRouteMapName	1.3.6.1.4.1.2272.1.80.1.1.2.1.7	6.0
rcMsdpPeerOutSAFilterEnabled	1.3.6.1.4.1.2272.1.80.1.1.2.1.8	6.0
rcMsdpPeerOutSAFilterRouteMapName	1.3.6.1.4.1.2272.1.80.1.1.2.1.9	6.0
rcMsdpSACacheRecordsTable	1.3.6.1.4.1.2272.1.80.1.1.4	6.0
rcMsdpSACacheRecordsEntry	1.3.6.1.4.1.2272.1.80.1.1.4.1	6.0
rcMsdpSACacheRecordsTypeInformation	1.3.6.1.4.1.2272.1.80.1.1.4.1.1	6.0
rcMsdpSACacheRecordsGroupAddr	1.3.6.1.4.1.2272.1.80.1.1.4.1.2	6.0
rcMsdpSACacheRecordsSourceAddr	1.3.6.1.4.1.2272.1.80.1.1.4.1.3	6.0
rcMsdpSACacheRecordsOriginRP	1.3.6.1.4.1.2272.1.80.1.1.4.1.4	6.0
rcMsdpSACacheRecordsOriginatorAsNumber	1.3.6.1.4.1.2272.1.80.1.1.4.1.5	6.0
rcMsdpSACacheRecordsRouteType	1.3.6.1.4.1.2272.1.80.1.1.4.1.6	6.0
rcMsdpNotificationObjects	1.3.6.1.4.1.2272.1.80.1.2	6.0
rcMsdpSACacheType	1.3.6.1.4.1.2272.1.80.1.2.1	6.0
rcMsdpVrfId	1.3.6.1.4.1.2272.1.80.1.2.2	6.0
rcMACSecConnectivityAssociationTxKeyParity	1.3.6.1.4.1.2272.1.88.1.1.6	6.0

Obsolete MIBs

Object Name	Object OID	Obsolete in Release
rcMsdpSACacheStatsClear	1.3.6.1.4.1.2272.1.80.1.1.1.5	6.0
rcPortBpduFilteringTimerCount	1.3.6.1.4.1.2272.1.4.10.1.1.69	6.0