



Release Notes for VSP 8600

Release 6.2 (VSP 8600)
9035568 Rev.02
December 2018

© 2017-2018, Extreme Networks
All Rights Reserved.

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: 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: <https://extremeportal.force.com/ExtrLicenseLanding> 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](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](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: www.extremenetworks.com/documentation/, or such successor site as designated by Extreme Networks.

Contact Extreme Networks Support

See the Extreme Networks Support website: 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 the support phone number in your country, visit: 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: www.extremenetworks.com/company/legal/

Contents

Chapter 1: Preface	6
Disclaimer.....	6
Purpose.....	6
Training.....	6
Providing Feedback to Us.....	7
Getting Help.....	7
Extreme Networks Documentation.....	8
Subscribing to Service Notifications.....	8
Chapter 2: New in this release	9
New in this Release.....	9
Filename for this Release.....	13
Chapter 3: Upgrade Paths and Considerations	15
Supported Upgrade Paths.....	15
Upgrade Considerations.....	15
IS-IS Authentication.....	15
Downgrade Considerations.....	16
Real Time Clock.....	16
MACsec on 100 Gb Devices.....	17
Software Version Mismatch Generates Warning Messages when Installing a New IOC Module...	17
Chapter 4: VSP 8600 Series Hardware and Software Compatibility	18
Chapter 5: Software Scaling	19
Layer 2.....	19
IP Unicast.....	19
Layer 3 Route Table Size.....	21
IP Multicast.....	21
Filters, QoS, and Security.....	21
Fabric Scaling.....	22
OAM and Diagnostics.....	22
Chapter 6: Important Notices	24
8624XS IOC Module Power Consideration.....	24
Feature Licensing.....	24
High Availability (HA).....	26
Network Load Balancing (NLB).....	26
System Name Prompt vs. IS-IS Host Name.....	26
VRRP IDs.....	26
Chapter 7: Known Issues and Restrictions	28
Known Issues and Restrictions.....	28
Filter Restrictions and Expected Behaviors.....	35
Chapter 8: Resolved Issues	38

Appendix A: Related Information	40
Features by Release.....	40
New MIBs.....	55

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

This document includes the following information:

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

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 <https://www.extremenetworks.com/documentation-feedback/>. You can also email us directly at documentation@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.
- **[Extreme Portal](#)** — Search the GTAC knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
- **[The Hub](#)** — A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

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 earlier 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/open-source-declaration/.

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

New in this Release

The following sections detail what is new in VSP 8600 Release 6.2. For a full list of features, see [Features by Release](#) on page 40.

New Hardware

VSP 8600 Series 6.2 introduces support for the following hardware:

Adapters:

- QSFP+ to SFP+ Adapter (PN: QSFP-SFPP-ADPT) — Can be used in QSFP+ ports to support SFP+ optical transceivers.
- QSFP28 to SFP28 Adapter (PN: 10506) — Can be used in QSFP+ ports for SFP+ transceivers or in SFP28 ports for SFP28 transceivers.

Direct-Attach Cables:

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

* Note:

In this release, support for 25 Gb optics and active and direct-attach cables are only supported on 100 Gb channelized ports with the QSFP28 to SFP28 Adapter.

25 Gb Pluggables:

- 25 Gb SR SFP28 (PN: 10501)
- 25 Gb SR-Lite MMF (Multimode Fiber) SFP28 (PN: 10502)
- 25 Gb ESR SFP28 (PN: 10503)
- 25 Gb LR 10 km SFP28 (PN: 10504)

! Important:

You must enable FEC to achieve proper functionality when using interconnects such as the 25 Gb SR, 25 Gb SR-lite, 25 Gb ESR optics or the 25 Gb AOC and 25 Gb DAC cables.

For more information:

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

Extreme Networks optical transceivers and components	Extreme Networks Pluggable Transceivers Installation Guide on the Extreme Networks documentation web site
Compatibility for Extreme Networks SFP, SFP+, QSFP+, and QSFP28 transceiver modules with the VSP series switches	VSP Components: SFP, SFP+, QSFP+, QSFP28 Support
Optical transceivers and components previously branded as Avaya	<i>Installing Transceivers and Optical Components on VSP Operating System Software</i>

256-bit MACsec on the 100 Gbps 8606CQ Module

This release introduces support for 256-bit MACsec on the 100 Gbps 8606CQ module. You can now configure the GCM-AES-256 with a maximum key length of 256 bits. This new feature is in addition to the existing GCM-AES-128 with a maximum key length of 128 bits. The default cipher suite is the GCM-AES-128.

For more information, see *Configuring Security*.

Application Telemetry

Application Telemetry is an analytics solution that combines the Deep Packet Inspection capabilities of Extreme Analytics Engine with sFlow data. This feature provides granular visibility into your network and monitors application performance, users, locations, and devices without the need for expensive sensors or collectors.

Application Telemetry uses policy rules to filter packets for analysis. This methodology enables Application Telemetry to monitor *all* application-level traffic flows at wire speed on *all* interfaces simultaneously.

For more information, see *Monitoring Performance*.

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*.

Channelization on the 8606CQ Module

This release introduces channelization support on all 100 Gbps ports on the 8606CQ module. Channelization enables you to configure 100 Gbps ports to operate as four 25 Gbps ports if QSFP28 transceivers are used or four 10 Gbps ports if QSFP+ transceivers are used.

DEMO FEATURE — HA CPU for Layer 2 Features with Simplified vIST

High Availability [HA] support in Simplified vIST configurations enable Layer 2 applications supported in Simplified vIST to be in sync between standby CPU and master CPU to provide hot standby capability (HA mode).

! Important:

HA CPU for Layer 2 Features with Simplified vIST is a demo feature. Do not use this feature in production environments.

For more information, see *Administering*.

Forward Error Correction (FEC)

This release introduces support for the configuration of Forward Error Correction (FEC) on the 100 Gbps ports of the 8606CQ module. You can also configure FEC on a channelized 100 Gbps port operating at 25 Gbps speed. FEC is useful for enhanced error correction when transmitting data over a noisy channel.

* Note:

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

Handling of IPv4 L-2 unicast packets at VRRP Backup-Master

For VSP 8600 6.2 and VOSS 7.1 releases and later, the handling of IPv4 Layer 2 unicast packets (for example, ARP Request/Reply) with the destination MAC as VRRP MAC has been modified on Backup-Master. These packets are now handled by VRRP Master only.

The Backup-Master forwards all IPv4 Layer 2 unicast packets to the Master and the Master VRRP sends an ARP reply only.

Processing of IP unicast packets (for example, ICMP packets to VRRP IP) or IPv4 routed packets (with destination MAC as VRRP MAC) on VRRP Backup-Master stays the same. For example, the VRRP Backup-Master replies to ICMP requests and routes Layer 3 routed packets to the destination and does not forward these packets to the Master when they arrive at the Backup-Master.

To reflect the above changes, the VRRP MAC entry on the Backup-Master now points to the Master instead of itself, and the ARP entry for VRRP IP on the backup-master points to local.

IPv6 Routing

Release 6.2 introduces support for IPv6 routing:

- Dual-Stack IPv4/IPv6 support
- 6in4 configured tunnels—This feature enables you to transition from an IPv4 network to an IPv6 network. The software supports 16 manually-configured 6in4 tunnels per chassis.

* Note:

6in4 tunnels are not supported if the tunnel source IP address is reachable through an IPv4 Shortcuts route.

- IPv6 Routing (Static, OSPFv3)
- VRRPv3 and IPv6 support on SMLT/RSMLT links—This feature enables you to design resilient IPv6 networks. The switch supports up to eight VRRP VRIDs for IPv4 and IPv6 (combined).

- IPv6 connectivity for management protocols—This feature enables RADIUSv6, DHCPv6, DNSv6, and Syslog servers in an IPv6 network.
- IPv6 OAM support—This feature includes support for Ping, Traceroute, Telnet, FTP, TFTP, Rlogin, SSH, SNMPv3, and EDM access via IPv6 HTTPS.
- IPv6 Access Control Lists (ACLs)—This release adds support for IPv6 ingress QoS ACLs and IPv6 *ingress security* ACL/Filters for ports and VLANs. It does not support the following:
 - IPv6 egress security ACL/Filters
 - IPv6 egress QoS ACL/Filters

For more information, see *Configuring QoS and ACL-Based Traffic Filtering*.

- IPv6 Routing provides partial HA support. The application synchronizes the static configuration from the master CPU to the standby CPU. However, the dynamic data learned by protocols are not synchronized.
- IPv6 Routing has the following restrictions:
 - The software does not support IPv4-mapped IPv6 addresses, for example, 0::FFFF:a.b.c.d, or IPv4-compatible IPv6 addresses, for example, 0::a.b.c.d.
 - The neighbor entry state on the CP and hardware cannot be synchronized. In some cases the neighbor entry to which traffic is forwarded may be shown as stale on the CP.
 - The switch does not support the IPv6 Path MTU feature.
 - The switch supports three IPv6 interface MTU values: 1280, 1500, and 9500.

*** Note:**

The `ipv6-mode` and `urpf-mode` boot flags are not applicable to the VSP 8600.

IP Multicast over Fabric Connect

Extreme Networks is leading the industry with a unique approach for IP multicast routing using IP Multicast over Fabric Connect. IP Multicast over Fabric Connect greatly simplifies multicast deployment, with no need for any multicast routing protocols such as Protocol Independent Multicast-Sparse Mode (PIM-SM) or Protocol Independent Multicast-Source Specific Multicast (PIM-SSM). A BEB can forward a multicast stream anywhere in an SPBM network where IS-IS advertises the stream to the rest of the fabric.

For more information, see *Configuring Fabric Multicast Services*.

QoS ACEs

This release supports Quality of Service (QoS) filter rules that you define with Access Control Entries (ACE). An ACE, which is contained in an Access Control List (ACL), provides match criteria and rules for ACL-based filters. An ACE can provide actions such as dropping a packet, monitoring a packet, or remarking QoS on a packet.

For more information, see *Configuring QoS and ACL-Based Traffic Filtering*.

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*.

SLPP Guard

Use SLPP Guard with Split Multi-Link Trunking (SMLT) to provide additional loop protection to protect wiring closets from erroneous connections. When you enable SLPP for SMLT configurations, the switch transmits SLPP-PDU packets to help prevent loops from occurring. When you enable SLPP Guard, the software extends this loop prevention mechanism to individual edge access ports. If the edge switch with SLPP Guard enabled receives an SLPP-PDU packet on a port, the switch disables the port operationally, and generates a log messages and SNMP trap.

For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST*.

Filenames for this Release

Important:

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

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

The following table provides the filenames and sizes for this release.

Table 1: Software Filenames and Sizes

Description	VSP 8600 Series	File size
SHA512 Checksum files	VOSS8600.6.2.0.0.sha512	1,409 bytes
MD5 Checksum files	VOSS8600.6.2.0.0.md5	545 bytes
MIB - supported object names	VOSS8600.6.2.0.0_mib_sup.txt	998,391 bytes
MIB - zip file of all MIBs	VOSS8600.6.2.0.0_mib.zip	1,086,882 bytes
MIB - objects in the OID compile order	VOSS8600.6.2.0.0_mib.txt	7,208,517 bytes
EDM plug-in for COM	VOSS86v6.2.0.0.zip	5,605,633 bytes
EDM Help files	VOSS86v620_HELP_EDM_gzip.zip	3,968,230 bytes
Logs reference	VOSS8600.6.2.0.0_edoc.tar	64,532,480 bytes
Software image	VOSS8600.6.2.0.0.tgz	149,525,288 bytes

The following table provides the open source software filenames and sizes for this release.

Table 2: Open Source Software Files

Master copyright file	Open source base software
VOSS8600.6.2.0.0_oss-notice.html 2,526,400 bytes	VOSS8600.6.2.0.0_OpenSource.zip 95,862,435 bytes

New in this release

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

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

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

Chapter 3: Upgrade Paths and Considerations

This section describes the upgrade path and any considerations that you should be aware of.

Supported Upgrade Paths

Validated upgrade paths are VSP 8600 Series 4.5.x or 6.1 to VSP 8600 Series 6.2.

At the time of publishing this document, there were no known restrictions on upgrades. Customers can upgrade directly from other releases to this release.

Upgrade Considerations

The *Administering* document includes detailed image management procedures that includes information about the following specific upgrade considerations:

- Pre-upgrade instructions for IS-IS metric type
- Upgrade considerations regarding MACsec replay-protect configuration
- Upgrade considerations for IS-IS enabled links with HMAC-MD5 authentication
- TACACS+ upgrade consideration

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

IS-IS Authentication

If you already have IS-IS Authentication enabled and then upgrade to Release 6.2, the IS-IS adjacencies may not get established. This issue affects the 100 Gb 8606CQ links only, but it can result in traffic loss.

Use the following procedure as a workaround:

1. Disable IS-IS Authentication on 100 Gb ports on both peers.
2. Update the software to Release 6.2.
3. Re-enable IS-IS Authentication.

*** Note:**

If you want to downgrade from Release 6.2, use this same procedure except specify the appropriate release in step 2.

Downgrade Considerations

Before you downgrade to an earlier software release, note the following downgrade considerations.

Real Time Clock

The latest VSP 8600 IOC modules have an updated real time clock (RTC) component, which is not compatible with some older software releases. The new modules should only be installed in a switch or chassis running the minimum supported software, which is 6.2.0.0.

Commissioning New RTC-updated Hardware

To determine if your hardware contains the updated RTC, use the `show sys-info card` command and check the H/W Revision field. If the IOC Module CardHWRevision is 14 or higher, then you have the updated RTC. With the updated RTC, you can only run 6.2.0.0 or higher software versions.

If you attempt to hot insert the latest IOC module (RTC updated) in a chassis running an older unsupported release, the IOC does not become operational. This card attempts to boot unsuccessfully and powers off after 5 boot attempts.

Downgrading New RTC-updated Hardware

If your chassis has any module with the new RTC component, you cannot downgrade the software to a version less than 6.2.0.0. During `software activate` execution, the switch prevents the downgrade and displays the following message:

```
ERROR: Hardware (revision 14) in slot <slot_number> is not supported in
this release. Cannot activate release <x.x.x.x>. Please refer to the
release notes or contact support.
```

If your chassis requires a software downgrade, you must remove all modules with the new RTC component from the chassis first.

*** Note:**

Removing these cards also results in a loss of configuration for the removed slots following a chassis boot.

MACsec on 100 Gb Devices

When two VSP 8606CQ modules are connected back to back, the MACsec connection works only if the software version on both ends are the same. The modules must be running either Release 6.1.x or 6.2.x. If one end has 6.1.x and the other end has 6.2.x, MACsec will not work and traffic will drop.

With this new implementation of MACsec on the 100 Gb 8606CQ module, the MACsec statistics increment the `Unchecked Packets` counter on the receiving link and not the `Accepted` or `Validated` counter. This counter issue happens only when encryption is disabled on both the transmitting and receiving links.

Software Version Mismatch Generates Warning Messages when Installing a New IOC Module

When there is a mismatch between the software running on the switch and the software on the IOC module, the switch updates the IOC module to the version of software running on the switch. During this process you see errors that are similar to the following:

```
IO1 [12/06/17 11:50:43.513:UTC] 0x0024854b 00000000 GlobalRouter SF-APP WARNING
FabDrv_lc::mapLocalPortsToSysports dnxBcm_assignSysPortToModPort failed: unit=0 sysport=0
modId=40000 tmPort=1
IO1 [12/06/17 11:50:43.526:UTC] 0x0024854b 00000000 GlobalRouter SF-APP WARNING
FabDrv_lc::configIngressSideVOQs: UNKNOWN PORT TYPE OF 773 localPort = 1 modId = 6
IO7 [12/06/17 11:50:45.673:UTC] 0x0024854b 00000000 GlobalRouter SF-APP WARNING
FabDrv_lc::createVoqsForPort: dnxBcm_setPacketLengthAdjustForVog failed: unit=0
voqBaseId=80000512 cos=4 PACKET_LENGTH_ADJUST=0
IO7 [12/06/17 11:50:45.688:UTC] 0x0024854b 00000000 GlobalRouter SF-APP WARNING
map_local_port_to_connectorPort: INVALID LOCAL PORT OF 10000000
```

The messages stop once the update of the IOC module software has completed. This has no impact on the switch operation.

Note:

This issue applies only to a switch running a mix of releases. For example, there is a mismatch if the switch is running release 6.1.x or higher and it has an IOC running release 4.5.x.

Chapter 4: VSP 8600 Series Hardware and Software Compatibility

Part number	Model number	Initial release	Supported new feature release			
			4.5.0.0	4.5.0.1	6.1	6.2
EC8602001-E6	VSP 8608	4.5.0.0	Y	Y	Y	Y
EC8602002-E6	VSP 8608 with 3 SF modules and 4 AC PSUs	4.5.0.0	Y	Y	Y	Y
EC8602003-E6	VSP 8608 DC with 3 SF modules and 4 DC PSUs	4.5.0.0	Y	Y	Y	Y
EC8604001-E6	8600SF	4.5.0.0	Y	Y	Y	Y
EC8604002-E6	8624XS	4.5.0.0	Y	Y	Y	Y
EC8604003-E6	8624XT	4.5.0.0	Y	Y	Y	Y
EC8604004-E6	8616QQ	4.5.0.0	Y	Y	Y	Y
EC8604005-E6	8606CQ	4.5.0.1	N	Y	Y	Y

Chapter 5: Software Scaling

This section lists software scaling capabilities for the VSP 8600 Series.

Layer 2

Table 3: Layer 2 Maximums

LACP aggregators	192 (up to 224 with channelization)
Layer 2 VSNs	4,000
MAC table size	256,000
MAC table size (with Switch Clustering)	128,000
Microsoft NLB cluster IP interfaces	200
MLT groups	192 (up to 224 with channelization)
MSTP instances	64
Port-based VLANs	4,059
Ports per LACP aggregator	8
Ports per MLT group	8
RSTP instances	1
SLPP VLANs	500
VLACP interfaces	128

IP Unicast

Table 4: IP Unicast Maximums

BGP+ peers	256
DHCP Relay forwarding entries (IPv4 or IPv6)	512 per VRF/1,024 per switch
ECMP groups/paths per group	1,000/8

Table continues...

IP interfaces (IPv4 or IPv6 or IPv4+IPv6)	4,059
IPv4 ARP table	64,000
IPv4 BGP peers	256
IPv4 CLIP interfaces	64
IPv4 RIP interfaces	200
IPv4 route policies (per VRF/per switch)	2,000/16,000
IPv4 static ARP entries (per VRF/per switch)	2,000/10,000
IPv4 static routes (per VRF/per switch)	2,000/10,000
IPv4 UDP forwarding entries	1,024
IPv4 VRF instances	512*
* NOTE : The maximum number of VRFs for inter-VRF redistribution is 256.	
IPv6 CLIP interfaces	64
IPv6 Ingress ACEs (Security and QoS)	2,000
IPv6 Neighbor table	16,000
IPv6 OSPFv3 routes - GRT only	32,000
IPv6 RIPng peers	48
IPv6 RIPng routes	16,000
IPv6 Route Table size	32,000
IPv6 static neighbor records	1,000
IPv6 static routes	10,000
Layer 3 VSNs	512
OSPF virtual instances	64
OSPF v2/v3 neighbors (active/passive)	500/2,000
OSPFv2 areas	12 per VRF or GRT/80 per switch
OSPFv3 areas	64
Routed Split Multi-LinkTrunking (RSMLT) interfaces	1,000
VRRP interfaces (IPv4 or IPv6)	512
VRRP interfaces with fast timers (200ms)	24
VRRP VRIDs	8 (combined across IPv4 and IPv6)
Manually configured 6-in-4 tunnels	16

Layer 3 Route Table Size

Table 5: Layer 3 Route Table Size Maximums

IPv4 BGP routes (control plane only)	1.5 M
IPv4 OSPF routes	64,000
IPv4 RIP routes (per VRF/per switch)	2,000/16,000
IPv4 routes	252,000
IPv4 SPB Shortcut routes	16,000

IP Multicast

Table 6: IP Multicast Maximums

IGMP interfaces	4,000
PIM interfaces (Active/Passive)	512/3,000
Multicast receivers/IGMP receiver entries (per switch)	6,000*
<p>* Note: 6000 is the the total number of unique SGVs for which there are receivers. The total number of receivers can be greater than 6000 if there are multiple receivers for the same group.</p>	
Multicast senders/IGMP sender entries (per switch)	6,000
PIM-SSM static channels	4,000
Total multicast routes (S,G,V) (per switch)	6,000

*** Note:**

IPv4 Routes, IPv4 SGV sender records, IPv6 Routes and IPv6 neighbor records reside in the same shared hardware table. If records of all 4 types are present together in this shared table, then the actual numbers that can be supported might be less than the scaling numbers indicated in the above tables.

Filters, QoS, and Security

Table 7: Filters, QoS, and Security Maximums

Total ACE - Ingress	3,500 (2,000 IPv4 ACEs and 1,500 IPv6 ACEs)
---------------------	---

Table continues...

Total ACE - Egress	2,000
Total ACL - Ingress	2,000
Total ACL - Egress	1,000

Fabric Scaling

Table 8: Fabric Scaling Maximums

Number of SPB regions	1
Number of B-VIDs	2
Number of SPB adjacencies	192
SPBM enabled nodes per region (BEB + BCB)	2,000*
* NOTE : If there are VSP 4000 switches in the network, then the total number of SPBM enabled switches per region is reduced to 550.	
Maximum number of IP multicast S,Gs when operating as a BCB	50,000
Number of BEBs this node can share services with (Layer 2 VSNs, Layer 3 VSNs, Multicast)	500**
** NOTE : vIST clusters are counted as 3 nodes.	
Maximum number of SPB Layer 2 multicast UNI I-SIDs	6,000
Maximum number of SPB Layer 3 multicast UNI I-SIDs	6,000
Maximum number of IP multicast S,Gs when operating as a BCB	50,000

OAM and Diagnostics

Table 9: OAM and Diagnostics Maximums

EDM sessions	5
FTP sessions	4
Mirrored destination ports	4
Mirroring ports	191
Rlogin sessions	8
sFlow sampling rate	5000 samples per second per IOC module

Table continues...

SSH sessions	8
Telnet sessions	8

Chapter 6: Important Notices

This section provides important information for this release.

8624XS IOC Module Power Consideration

1 Gbps or 10 Gbps copper transceivers in any port of the 8624XS IOC module continue to receive power even after you enter the `no sys power slot` command. This causes the remote end to declare the port UP and send traffic.

*** Note:**

This issue can cause a problem *only* if you use the `no sys power slot` command locally to power down and leave the module in the slot. Although all the ports are initially brought down gracefully as part of the execution of `no sys power slot`, the ports with 1 Gbps or 10 Gbps copper transceivers continue to receive power locally causing the PHY in the transceivers to renegotiate with the remote port. Eventually the port will be declared UP in the remote end. However, the local end will still stay operationally down. Traffic loss results when the remote switch tries to send traffic to these ports.

To resolve this issue, use one of the following workarounds:

- Shut down the ports (`shutdown port`) in the remote switch before issuing the `no sys power slot` command locally.
- Configure VLACP on the links connected through the copper transceivers above if the far end switch supports VLACP. This provides a logical link down notification at the far end and prevents traffic loss.
- Remove the local IOC module that was powered down.


Feature Licensing

Licensing allows switch operators to select the features that best suits their needs.

The VSP 8600 Series supports a licensing model that has two main categories of licenses: Base License and Feature Pack Licenses. A Base License enables base software features and one is

required per IOC in the chassis. You require a Feature Pack License to enable additional features that are grouped into Feature Packs. These licenses are optional.

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

Offer Level	Period	Support
Factory Default	30-days	Can configure all features, excluding MACsec.
Trial	60 days	<p>Can test licensed features. The following types of Trial Licenses are available:</p> <ul style="list-style-type: none"> allows the use of all features excluding MACsec allows the use of all features including MACsec <p> Note: You can activate a Trial License once per switch.</p>
IOC Base License		<p>Can use Base software features on the switch.</p> <p>IOC Base license is required for each IOC module that you plan to install in the chassis. If the number of IOCs exceeds the licensed IOC quantity, the ports on the excess IOCs are license-locked and appear administratively down.</p>
Feature Pack		<p>Features that are not available in the Base License are grouped into Feature Packs based on use case. A license is required to use a Feature Pack. A Feature Pack License applies to the entire chassis; you do not need to purchase this license type for each installed IOC module.</p> <p>Feature Pack licenses that the VSP 8600 supports:</p> <p>Layer 3 Virtualization:</p> <ul style="list-style-type: none"> Layer 3 Virtual Services Networks (VSNs) Greater than 24 VRFs Greater than 16 BGP Peers <p>Layer 3 Virtualization with MACsec:</p> <ul style="list-style-type: none"> Layer 3 Virtual Services Networks (VSNs) Greater than 24 VRFs Greater than 16 BGP Peers MACsec

For more information about licenses, see *Administering*.

High Availability (HA)

VSP 8600 supports controller redundancy, thus enabling High Availability (HA). Each IOC module supports both I/O and supervisor/controller functionality. An IOC inserted in Slot 1/2 acts as the Master/Standby Controller in an HA configuration.

VSP 8600 supports two HA modes: Warm Standby and Hot Standby.

- In Warm Standby mode, the configurations are synchronized between Master and Standby IOCs. In Warm Standby mode, if there is a software failure on the Master IOC, the Standby IOC immediately takes over and reboots all the other IOCs. If Fabric or vIST is provisioned, non-stop forwarding can be achieved by network-based resiliency enabled by these technologies.
- In Hot Standby mode, both configuration and protocol states are synchronized between Master and Standby, thus ensuring a hitless switchover upon Master IOC failure.

 **Important:**

Hot Standby does not support configurations with SPBM, vIST, or SMLT.

Network Load Balancing (NLB)

VSP 8600 supports Network Load Balancing (NLB) in Unicast mode only.

System Name Prompt vs. IS-IS Host Name

Starting with Release 6.1, the software no longer allows spaces in the system name prompt, but it still allows spaces in the IS-IS host name. When you upgrade, the software replaces spaces in the system name with underscores while leaving the IS-IS host name unchanged.

VRRP IDs

Because there is a hardware limitation of using only eight MAC addresses for VRRP, the number of VRIDs is also limited to eight. You can use any eight values for VRIDs between 1 and 255. However, once you choose the eight VRID values, you must reuse the same eight values across all VLANs on the device.

As VRRP virtual MAC for IPv4 and IPv6 for a same VRID is different, IPv4 and IPv6 VRRP instance with same VRID will consume 2 VRRP MAC entries. For example: if VRID 1 is used for IPv4 and IPv6 is used, virtual MAC for IPv4 and IPv6 are 00:00:5e:00:01:01 and 00:00:5e:00:02:01 respectively. These virtual MAC addresses use 2 VRRP MAC addresses in hardware.

Using the syntax for establishing the VRID and Virtual IP Address (`ip vrrp address [VRRP ID] [VRRP Virtual IP Address]`), the following example uses VRIDs from 2 through 9. This example shows only the relevant commands to illustrate this issue.

```
VSP8600:1(config-if)#ip vrrp address 2 2.1.1.10
VSP8600:1(config-if)#ip vrrp address 3 3.1.1.10
VSP8600:1(config-if)#ip vrrp address 4 4.1.1.10
VSP8600:1(config-if)#ip vrrp address 5 5.1.1.10
VSP8600:1(config-if)#ip vrrp address 6 6.1.1.10
VSP8600:1(config-if)#ip vrrp address 7 7.1.1.10
VSP8600:1(config-if)#ip vrrp address 8 8.1.1.10
VSP8600:1(config-if)#ip vrrp address 9 9.1.1.10
```

At this point you have used all the VRIDs in the selected range (2–9). Now you must start reusing the VRIDs from 2 to 9 for all other VRRP enabled VLANs. The following example shows what happens when you do not reuse a VRID from the selected range.

```
VSP8600:1(config-if)#ip vrrp address 10 10.1.1.10
Error: maximum number of VRRP entries exceeded
```

The following example shows the correct reuse of one of the VRIDs from the selected range.

```
VSP8600:1(config-if)#ip vrrp address 2 10.1.1.10
```

Chapter 7: Known Issues and Restrictions

This section details the known issues and restrictions found in this release.

Known Issues and Restrictions

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

General Issues and Restrictions

Issue number	Description	Workaround
VOSS-4712	When there are broadcast packets in the VLAN, these packets are sent to all ports in the VLAN. The packets get dropped because the port is operationally down. However, outPkts stats increment and the unicast packets are not sent to that port because the port is down.	Ignore the stats counter when port is down.
VOSS-5191	The OSPF MD5 related functionality cannot be enabled from EDM.	Use CLI to configure OSPF MD5 related functionality.
VOSS-5511	Half duplex option is not supported, but it can be configured on VSP 8600 port.	Do not configure half-duplex.
VOSS-5702	Multicast traffic will not have DSCP marked (when enabled on incoming port), when IGMP snooping is enabled on the VLAN.	No workaround.
VOSS-5990	Path MTU discovery feature is not supported for IPv6. Due to this, packets larger than IPv6 interface MTU size are dropped but no ICMP error message is sent to the source host indicating the reason for this drop.	No workaround.
VOSS-6102	<code>sys action reset counters</code> command does not reset ISIS control packets.	Use <code>clear isis</code> command to reset stats.
VOSS-6103	<code>sys action reset counters</code> command does not reset ISIS int-counters.	Use <code>clear isis</code> command to reset stats.
VOSS-6104	<code>sys action reset counters</code> command does not reset any ISIS system stats.	Use <code>clear isis</code> command to reset stats.

Table continues...

Issue number	Description	Workaround
VOSS-7148	EDM: In the Virtual IF tab, the options SHA-1 and SHA-2 are not available to configure virtual link authorization.	Use CLI to configure virtual link authorization.
VOSS-7179	EDM: Device Physical View tab displays the power supplies but does not show their LED status to determine if it is AC, DC or in a failed state.	In EDM, navigate to Edit > Power Supply tab to check the power supply status.
VOSS-7500	COM+ does not display correct number of IP OSPF ECMP routes.	Use CLI and EDM to check IP OSPF ECMP routes.
VOSS-7709	On the 8608CQ IOC module, the output of the show interface gigabitEthernet statistics command does not display a value in IN PACKET for packets that have ethertype/length field of 0.	No workaround.
VOSS-7713	The system does not currently restrict the number of NLB virtual IP address ARP entries learned. The following message is logged but does not prevent the addition of new entries in the ARP table: <pre>CP1 [09/15/17 11:34:20.192:EDT] 0x0003c984 00000000 GlobalRouter IP WARNING rcIpAddArp: Maximum number of NLB servers supported has been reached. New NLB server connection requests are ignored.</pre>	No workaround. Do not scale beyond the documented scaling number of 200 NLB servers in a cluster.
VOSS-7941	When there is a mismatch between the software running on the switch and the software on the IOC module, the switch updates the IOC module to the version of software running on the switch. During this process you see errors that are similar to the following: <pre>IO1 [12/06/17 11:50:43.513:UTC] 0x0024854b 00000000 GlobalRouter SF-APP WARNING FabDrv_lc::mapLocalPortsToSysports dnxBcm_assignSysPortToModPort failed: unit=0 sysport=0 modId=40000 tmPort=1 IO1 [12/06/17 11:50:43.526:UTC] 0x0024854b 00000000 GlobalRouter SF-APP WARNING FabDrv_lc::configIngressSideVOqs: UNKNOWN PORT TYPE OF 773 localPort = 1 modId = 6 IO7 [12/06/17 11:50:45.673:UTC] 0x0024854b 00000000 GlobalRouter SF-APP WARNING FabDrv_lc::createVoqsForPort: dnxBcm_setPacketLengthAdjustForVoq failed: unit=0 voqBaseId=80000512 cos=4 PACKET_LENGTH_ADJUST=0 IO7 [12/06/17 11:50:45.688:UTC] 0x0024854b 00000000 GlobalRouter SF-APP</pre>	No workaround, but there is no operational impact.

Table continues...


Issue number	Description	Workaround
	<p>WARNING map_local_port_to_connectorPort: INVALID LOCAL PORT OF 10000000</p> <p>The messages stop once the update of the IOC module software has completed. This has no impact on the switch operation.</p> <p> Note:</p> <p>This issue applies only to a switch running a mix of releases. For example, there is a mismatch if the switch is running release 6.1.x or higher and it has an IOC running release 4.5.x.</p>	
VOSS-8017	SNMPv3 privacy option supports DES and AES128 only. There is no support for higher AES options like AES192, AES256, and AES512.	No workaround.
VOSS-8110	CLI does not display the SSL certificate information.	No workaround.
VOSS-8278	EDM does not have a field to configure the RSA user key.	Use the CLI to configure the RSA user key.
VOSS-8444 VOSS-8758	Disabling IS-IS incorrectly may cause unforeseen problems including traffic loss.	Use the following procedure: <ol style="list-style-type: none"> 1. Shut down NNI ports first. 2. Disable IS-IS globally.
VOSS-8469	For Windows Server Certificate Authorities, the IPsec tunnel cannot use digital certificates as the authentication method.	Use EJBCA as the CA.
VOSS-8516	Secure Copy (SCP) cannot use 2048-bit public DSA keys from Windows.	Use 1024/2048-bit RSA keys or 1024-bit DSA keys.
VOSS-8549	Configuring inter-VRF redistribution on more than 256 VRFs may deplete virtual memory and cause the following warning: <pre>VmSize of proc cbcp-main.x(4429) is 1867272KB, above 90% of available 1782579KB(index 0).</pre>	Configure inter-VRF redistribution on a maximum of 256 VRFs.
VOSS-8831	When ingress mirroring is configured on an NNI port, two mirrored copies will be made for an incoming Mac-in-Mac packet that contains Multicast BMAC DA, and also if the ISID carried in the packet is terminated on that fabric connect node. <p>This issue is specific to IP Multicast over Fabric Connect only.</p>	No workaround.

Table continues...

Issue number	Description	Workaround
VOSS-9977	<p>Filter statistics do not increment if the incoming packet is marked for drop AND the filter has an action of mirror.</p> <p>For example:</p> <p>Packets may be marked for drop because the port is not a member of the VLAN specified in the packet. The mirror action does take place (along with other actions, if any, such as internalQos).</p> <p>Filter statistics increment normally if the packet is not marked for drop or if the packet does not contain a mirroring action (even if the packet is marked for drop).</p>	<p>If traffic is getting dropped because the port is not a member of the VLAN then make sure the port is part of the VLAN present in the packet.</p>
VOSS-9985	<p>If an IGMPv3 interface has both static and dynamic receivers on the same port, the switch clears the static port from the outgoing port list when the dynamic receiver disappears.</p> <p>To avoid this potential traffic loss, avoid having both static and dynamic receivers on an IGMPv3 interface.</p>	<p>No workaround.</p>
VOSS-10091	<p>After deleting an IPVPN, you may see the following error message: <code>ercdDeleteIpmcRecord:1734 ercdIpmcLookupAvlTree() failed SrcIp: 0x1b000093, DstIp: 0xe6290000 vlan_id 0xfff</code></p> <p>This issue has no impact on the switch operation.</p>	<p>No workaround.</p>
VOSS-10362	<p>There is no consistency check to prevent a user from assigning a new I-SID value to a VLAN that already has an I-SID assigned to it. This is currently the existing behavior for I-SID Assignment and users should be aware of this to prevent unintended consequences.</p>	<p>No workaround.</p>
VOSS-10473	<p>When you boot a configuration that has static MACs configured on MLT ports, the static MACs do not appear on the sVIST peer for 18.5 minutes.</p>	<p>Try any of the following workarounds:</p> <ul style="list-style-type: none"> • Delete and re-add the static MACs. • Enter the <code>vlan action 2 flushmacfdb</code> command on the sVIST peer. • Reboot sVIST peer - MAC count and static MACs are in sync with peer after boot. • Disable STP on MLT ports and reboot.

Table continues...

Known Issues and Restrictions

Issue number	Description	Workaround
		<ul style="list-style-type: none"> • Wait until the next IST sync happens.
VOSS-10544	<p>When booting the switch, you may see the following sync error: HW ERROR framework_process_entity_data: Application Sync failed for entity: 0x4d535450 representing Module MSTP ,event:6/5.</p> <p>This issue has no impact on the switch operation.</p>	No workaround.
VOSS-10557	SNMP Get tools do not translate the port number to a name.	To get the port name, use the CLI or EDM.
VOSS-10675	Multicast traffic loss is seen when you delete and recreate a VLAN with multicast interfaces. This occurs in a scaled setup with more than 2,000 routes and the next hop is in the recreated VLAN.	Remove the VLAN and then recreate it with all ports shut down.
VOSS-10681	<p>After deleting an L3VSN VLAN running IPMC traffic and then recreating it in the GRT (VRF 0), you may see OSAL backtrace messages such as the following:</p> <pre>1 2018-06-26T06:33:45.090-05:00 VSP8608-1(120.169) CP1 - 0x0022c590 - 00000000 GlobalRouter OSAL INFO [bt] Execution path: 1 2018-06-26T06:33:45.090-05:00 VSP8608-1(120.169) CP1 - 0x0022c590 - 00000000 GlobalRouter OSAL INFO [bt] /opt/ appfs/lib/cp/libndutl.so.1(nd_utl_backtrace+0x4c) [0xfc8ff20] 1 2018-06-26T06:33:45.090-05:00 VSP8608-1(120.169) CP1 - 0x0022c590 - 00000000 GlobalRouter OSAL INFO [bt] cbc- main.x(show_stackframe+0x1c) [0x1141c4f0]</pre> <p>This issue has no impact on the switch operation.</p>	No workaround.
VOSS-10802	<p>The show app-telemetry status command incorrectly displays the Collector status as <code>not reachable</code>.</p> <p>There is no functional impact with this issue and it occurs only in configurations where the sFlow collector is reachable through both the management port (MGMT) and GRT. sFlow can reach the collector through MGMT, but Application Telemetry does not route through MGMT. Application Telemetry routes through the GRT.</p>	Avoid configurations where the sFlow collector is reachable through both the MGMT and GRT.

Table continues...


Issue number	Description	Workaround
VOSS-10839	The <code>no mvpn enable</code> and <code>no ipvpn</code> commands could cause IS-IS adjacency flapping in setups with a large number of multicast streams and receivers. SPBM traffic cannot pass through the switch until the adjacencies are up again.	Use one of the following workarounds: <ul style="list-style-type: none"> • Increase the IS-IS hold down timer. • Remove the multicast streams or the multicast receivers in that VRF and then execute <code>no mvpn enable</code> or <code>no ipvpn</code>.
VOSS-10852	In an IP Multicast over Fabric Connect scenario with a local SMLT sender and A and B vIST peers, the multicast traffic is hashed to A on VLAN xxx. VLAN xxx is not yet configured on A and B. <ol style="list-style-type: none"> 1. Configure VLAN xxx with <code>ip spb-multicast enable</code> on A. The sender is created on A and tries to sync to B. However, B ignores the message since VLAN xxx is not yet configured on B. 2. Configure VLAN xxx with <code>ip spb-multicast enable</code> on B. The local senders on A are not sent to B until the periodic resync that occurs every 15 minutes. During this 15 minutes if an SMLT outage appears and traffic is hashed to B, there will be minimal traffic outage until B creates the distribution tree on the SPBM core. <p> Important: This issue happens only after deleting and re-adding already existing VLANs.</p>	Use one of the following workarounds: <ul style="list-style-type: none"> • Bounce IP Multicast over Fabric Connect on A's VLAN xxx. • Create VLAN xxx on A and B with no traffic running.
VOSS-10876	Application Telemetry reachability information is not available from EDM.	Check the logs or use the CLI <code>show app-telemetry status</code> command.
VOSS-11063 VOSS-10628	After deleting and re-creating (or swapping) primary and secondary B-VLANs in a scaled SPBM fabric network with a large number of flows, there might be some unicast and multicast traffic loss on some of the flows.	After deleting and re-creating the B-VLANs, if some of the traffic flows don't recover, then reboot the switch for all the traffic to resume.
VOSS-11071	If you toggle an SF or I/O module off and on (<code>sys power</code>) and perform a CP switchover in parallel (<code>sys action cpu-switch-over</code>), the <code>show sys-info</code> command displays the Power State as <code>Off</code> even though Oper status and Admin status are <code>UP</code> .	No workaround.

Table continues...

Known Issues and Restrictions

Issue number	Description	Workaround
	This issue has no impact on the switch operation and the card is powered OFF/ON correctly. After a few minutes' delay, the data re-syncs automatically between the two SF modules and the display is corrected.	
VOSS-11383	While the master CP on the VSP 8600 is crashing, if a remote port is brought up, the link status on the remote device is link UP but on the VSP 8600 the link status is DOWN.	Perform admin shutdown followed by no shutdown on the remote port.
VOSS-11414	When IS-IS routes are removed because the next hop is no longer present, you may see COP error messages like the following: COP-SW ERROR ercdProcIpRecMsg: Failed to Delete IP Record. IpAddr:3.0.34.160 IpMask: 255.255.255.224 vrfID:9 retStatus: -4 This issue has no impact on the switch operation and occurs only when an IS-IS accept policy has been applied.	No workaround, but there is no operational impact.
VOSS-11491	If you toggle VRRP mastership by deleting the VLAN I-SID configured on the master VRRP node, the VRRP master node does not respond to Unicast ARPs destined to the VRRP MAC address.	Toggle IP VRRP on the VLAN interface of both the VRRP Master and Backup nodes using the following commands: • no ip vrrp <vlan_id> enable • ip vrrp <vlan_id> enable
VOSS-11521	EDM does not display the Card HW Revision number correctly.	Use the CLI command show sys-info card to display the card's hardware revision information.
VOSS-11530	The hardware clock is only set on a reboot of the switch using the CLI. Power cycling (disabling and enabling power) of the switch will not write to the hardware clock.	No workaround.
VOSS-11537	The clock is usually changed or synced at boot time. Changing the time on the fly at runtime causes LLDP neighbors to bounce. VSP 8600 applications do not depend on LLDP so there is no impact other than seeing LLDP messages on the console or log file.	No workaround.
VOSS-11551	8606CQ with a channelized port using QSA28 adapter and 25gigDAC/optics occasionally do not pass traffic even when the physical link is up.	The port needs to be de-channelized and reconfigured to bring the port up and successfully

Table continues...

Issue number	Description	Workaround
		pass traffic. This includes control and data traffic.
VOSS-11744	If in the same unicast route change check interval, you configure the same static RP for some group ranges while the PIM neighbor to the RP address is down and then configure all other ranges when the PIM neighbor comes back up, some group ranges will show invalid states while others show valid states for the same static RP.	Use one of the following workarounds: <ul style="list-style-type: none"> • Delete the particular RP entry and readd it for certain group ranges. • Bounce the port towards the RP. • Bounce PIM on that particular interface.
VOSS-11743	In a simplified vIST Layer 3 configuration, where the vIST peers connect to access switch/host through an LACP mlt, access switch/host may not be able to ping vlan IP address of a vist switch that was rebooted or have a CPU switch-over. Problem corrects itself after the next periodic mac sync from vist peer.	Use one of the following workarounds: <ul style="list-style-type: none"> • Use the clear ip arp command on the switch having the issues. • Wait 8 minutes for the next vIST MAC/ARP sync across the vIST peers.
VOSS-11755	IP Shortcuts packets destined to terminating BEB's CP with ethertype=0x88a8 are not recognized as IP packets hence dropped and the Ping fails.	No workaround. Make sure that terminating BEB does not receive IP Shortcuts traffic with Ethertype 0x88a8.
VOSS-11756	If spbm ethertype is set to 0x88a8 on VSP 8600, which is a Transit BCB, then it updates ethertype for all outgoing packets on NNI port to 0x88a8. It should be changing this only for Mac-in-Mac encapsulated packets and not for IP Shortcuts packets.	No workaround. Reconfigure Ethertype to 0x8100.

Filter Restrictions and Expected Behaviors

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

The following list describes the expected behavior with filters:

- ACL: The incoming packets must be tagged to hit an entry of port-based ACLs containing a VLAN based qualifier in the ACE.
- ACL: InVlan ACLs can match tagged or untagged traffic, with the port-default VLAN considered if the incoming packet is untagged. However, if an ACE of an InVlan ACL contains the qualifier `vlan-tag-prio`, it can be used to filter only tagged traffic and not the untagged traffic.
- ACL: The outPort ACLs cannot match on the fields that are changed in the packet during forwarding decisions. Hence, the fields (Destination MAC, Source MAC, VLAN ID, etc.), which

get modified during Layer 3 routing, cannot be used to match on the new contents of these fields in the outgoing packet.

- ACL: The outPort ACLs cannot match on a destination port that is a member of an MLT. So if port 1/5 is a member of an MLT (static or via LACP), an ACE of an outPort filter with member 1/5 will not be hit.
- ACL: In an outPort ACL, the ACEs containing Layer 3 qualifiers will only be hit for packets that are routed. So the qualifiers such as `src-ip` and `dst-ip` (in the `filter acl ace ip <acl><ace>` command) does not work for Layer 2 switched packets.
- ACL: Each filter member port uses a separate TCAM entry, which impacts the overall ACE scaling number. For example, an inPort filter with 5 members that has one ACE configured uses 10 different TCAM entries (with at least 5 each for the user and default ACEs).
- ACL: For outPort ACLs, the use of the `ethertype` qualifier results in two TCAM entries being used internally instead of one (one each for single tagged and untagged packets). The packets with multiple tags are unsupported as we cannot match on Ethertype field of such packets. If VLAN qualifiers are present in ACE (for example, `vlan-id` or `vlan-tag-prio`), the entry for untagged packets is not created internally. So a single TCAM entry is used that matches the tagged packets alone. This impacts the overall ACE scaling number.
- There can be a single ACE hit for a packet. Port-based ACLs have precedence over VLAN based ACLs. However, the default ACEs have a lower priority than the user ACEs.
 1. User ACE of InPort ACL
 2. User ACE of InVlan ACL
 3. Default ACE of InPort ACL
 4. Default ACE of InVlan ACL

*** Note:**

If a packet matches a user ACE in both an inPort and inVLAN ACL, the inVLAN ACL is ignored.

If a packet matches a user ACE in VLAN-based ACL and the default ACE of an inPort ACL, the user ACE in the inVLAN ACL is hit and the inPort ACL is ignored.

- ACL: The monitor actions (`monitor-dst-port` or `monitor-dst-mlt`) are not supported for outPort ACLs. They are only applicable to Ingress ACLs (InPort or InVlan). For flow-based mirroring, you can configure these monitor actions at the ACE level.
- ACE: When an ACE with action count is disabled, the statistics associated with the ACE are reset.
- For ACEs of port-based ACLs, you can configure VLAN qualifiers. Configuring Port qualifiers are not permitted.

For ACEs of VLAN-based ACLs, you can configure port qualifiers. Configuring VLAN qualifiers are not permitted.

Filters and QoS

Note the following VSP 8600 filters:

- VSP 8600 does not support the following qualifiers in the egress direction (outPort). However, ingress support (inVlan/InPort) for these qualifiers are available.
 - `arprequest` and `arpresponse`
 - `ip-frag-flag`
 - `tcp-flags`
- The `ip-options` qualifier is not supported.
- The QoS ACE action `remark-dot1p` on ingress (for port and VLAN ACLs) is not supported.

For more information, see *Configuring QoS and ACL-Based Traffic Filtering*.

Chapter 8: Resolved Issues

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

Fixes from previous releases

VSP 8600 Series 6.2 incorporates all fixes from prior releases.

Resolved issues in VSP 8600 Series 6.2

Issue number	Description
VOSS-5797	Error message appears when SSIO process is terminated.
VOSS-7305	In a scaled setup, if thousands of ARP records are getting aged out at the same interval, the TTL value displayed in the show ip arp output can go to a negative value. This causes the ARP aging to get delayed.
VOSS-7380	The Management port supports 100/1000 full duplex speeds through auto-negotiation. 10 M half/full and 100 M half duplex speeds are not supported.
VOSS-8208	SCP is supported for RWA users only. RW or R level will not work and the switch logs a message on the device.
VOSS-8329	LED blinking in EDM is representative of, but not identical to, the actual LED blinking rates on the switch.
VOSS-8336	BGP+ with OSPFv3 route redistributed ingress traffic is dropped (IN_DISCARD) on a remote tunnel when the corresponding neighbor is in the Stale state. Egress traffic is processed with no issues.
VOSS-8412	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.
VOSS-8430	CLI and EDM do not display the MACsec cipher type that the switch is using.
VOSS-8765	OSPFv3 adjacencies are not coming up in a full mesh square SMLT environment.
VOSS-8872	<ul style="list-style-type: none"> • <code>show ipv6 neighbor interface</code> displays IPv6 neighbor entries for vIST peers as <code>DYNAMIC INCOMPLETE</code>. • Cannot ping the gateway IPv6 address in an SMLT environment.
VOSS-9142 VOSS-9148	In a scaled environment with IP Shortcuts enabled, if a number of layer 3 interfaces such as VLANs and ports associated with layer 3 VSNs that have a large number of routes removed, there is potential to have a temporary service

Table continues...

Issue number	Description
	interruption or unresponsive user interface. The system will recover without intervention.
VOSS-9380	Removing the IP address on an IGMP Snoop enabled VLAN disables IGMP Snooping in the data path and causes traffic loss. Traffic recovers immediately when you disable and re-enable snooping on the VLAN or reconfigure the IP address.

Appendix A: Related Information

The following section contains information related to the current release.

Features by Release

The following table identifies the release that first introduced feature support on the VSP 8600 Series. Each new release includes all the features from previous releases unless specifically stated otherwise.

Feature	Release
Access Control List (ACL)-based filtering: <ul style="list-style-type: none">• Egress ACLs• Ingress ACLs• Layer 2 to Layer 4 filtering• Port-based• VLAN-based For more information, see <i>Configuring QoS and ACL-Based Traffic Filtering</i> .	4.5
Address Resolution Protocol (ARP): <ul style="list-style-type: none">• Proxy ARP• Static ARP For more information, see <i>Configuring IPv4 Routing</i> .	4.5
Alternative routes for IPv4 For more information, see <i>Configuring IPv4 Routing</i> .	4.5
Alternative routes for IPv6 For more information, see <i>Configuring IPv6 Routing</i> .	6.2
Application Telemetry For more information, see <i>Monitoring Performance</i> .	6.2
Automatic QoS	4.5

Table continues...

Feature	Release
For more information, see <i>Configuring QoS and ACL-Based Traffic Filtering</i> .	
Border Gateway Protocol for IPv4 (BGPv4) For more information, see <i>Configuring BGP Services</i> .	4.5
BGP+ (BGPv4 for IPv6) For more information, see <i>Configuring BGP Services</i> .	6.2
BGPv6 For more information, see <i>Configuring BGP Services</i> .	n/a
Bridge Protocol Data Unit (BPDU) Guard For more information, see <i>Configuring VLANs, Spanning Tree, and NLB</i> .	6.2
Certificate order priority For more information, see <i>Configuring Security</i> .	n/a
CFM configuration on C-VLANs For more information, see <i>Troubleshooting</i> .	n/a
Channelization of 40 Gbps ports For more information, see the hardware documentation and <i>Administering</i> .	6.1
Channelization of 100 Gbps ports For more information, see the hardware documentation and <i>Administering</i> .	6.2
Command Line Interface (CLI) For more information, see <i>Configuring User Interfaces and Operating Systems</i> .	4.5
Differentiated Services (DiffServ) including Per-Hop Behavior For more information, see <i>Configuring QoS and ACL-Based Traffic Filtering</i> .	4.5
Digital Certificate/PKI For more information, see <i>Configuring Security</i> .	6.1
Directed Broadcast For more information, see <i>Configuring Security</i> .	n/a
Distributed Virtual Routing (DvR) controller For more information, see <i>Configuring IPv4 Routing</i> .	n/a

Table continues...

Related Information

Feature	Release
Distributed Virtual Routing (DvR) leaf For more information, see <i>Configuring IPv4 Routing</i> .	n/a
Domain Name Service (DNS) client (IPv4) For more information, see <i>Administering</i> .	4.5
DNS client (IPv6) For more information, see <i>Administering</i> .	6.2
Dot1Q MIB <ul style="list-style-type: none"> • dot1VlanCurrentTable • dot1qVlanStaticTable • dot1qPortVlanTable • dot1dBasePortEntry • dot1qVlanNumDelete 	6.1
Dynamic Host Configuration Protocol (DHCP) Relay, DHCP Option 82 For more information, see <i>Configuring IPv4 Routing</i> .	4.5
DHCP Snooping (IPv4) For more information, see <i>Configuring Security</i> .	n/a
DHCP Snooping (IPv6) For more information, see <i>Configuring Security</i> .	n/a
DHCPv6 Guard For more information, see <i>Configuring Security</i> .	n/a
Dynamic ARP Inspection (DAI) For more information, see <i>Configuring Security</i> .	n/a
Egress port mirror For more information, see <i>Troubleshooting</i> .	4.5
Egress port shaper For more information, see <i>Configuring QoS and ACL-Based Traffic Filtering</i> .	4.5
Encryption modules The encryption modules file is included in the runtime software image file; it is not a separate file.	4.5
Enhanced Secure mode for JITC and non-JITC sub-modes. For more information, see <i>Administering</i> .	n/a
EDM representation of physical LED status	4.5

Table continues...

Feature	Release
For more information, see <i>Installing the Virtual Services Platform 8600</i> .	
Entity MIB enhancements and integration for the following: <ul style="list-style-type: none"> • Physical Table • Alias Mapping Table • Physical Contains Table • Last Change Time Table For more information, see <i>Administering</i> .	6.1
Equal Cost Multiple Path (ECMP) for IPv4 For more information, see <i>Configuring IPv4 Routing</i> .	4.5
ECMP for IPv6 For more information, see the following documents: <ul style="list-style-type: none"> • <i>Configuring IPv4 Routing</i> • <i>Configuring BGP Services</i> • <i>Configuring IPv6 Routing</i> 	6.2
ECMP support for VXLAN Gateway and Fabric Extend For more information, see <i>Configuring VLANs, Spanning Tree, and NLB</i> .	n/a
Equal Cost Trees (ECT) For more information, see <i>Configuring Fabric Basics and Layer 2 Services</i> .	4.5
E-Tree and Private VLANs For more information about E-Tree, see <i>Configuring Fabric Basics and Layer 2 Services</i> . For more information about Private VLANs, see <i>Configuring VLANs, Spanning Tree, and NLB</i> . For information about how to configure MLT and Private VLANs, see <i>Configuring Link Aggregation, MLT, SMLT, and vIST</i> .	n/a
Extensible Authentication Protocol (EAP) and EAP over LAN (EAPoL) For more information, see <i>Configuring Security</i> .	n/a
EAPoL MHMA-MV For more information, see <i>Configuring Security</i> .	n/a

Table continues...

Related Information

Feature	Release
EAPoL enhancements: Enhanced MHMV, Fail Open VLAN, Guest VLAN For more information, see <i>Configuring Security</i> .	n/a
External BGP (EBGP) For more information, see <i>Configuring BGP Services</i> .	4.5
Extreme Management Center backup configuration ZIP file For more information, see Extreme Management Center documentation.	6.1
Fabric Attach For more information, see <i>Configuring Fabric Basics and Layer 2 Services</i> .	n/a
Fabric Attach Zero Touch Client Attachment For more information, see <i>Configuring Fabric Basics and Layer 2 Services</i> .	n/a
Fabric BCB mode For more information, see <i>Configuring Fabric Basics and Layer 2 Services</i> .	4.5
Fabric BEB mode For more information, see <i>Configuring Fabric Basics and Layer 2 Services</i> .	6.1
Fabric Connect services with switch cluster For more information, see the Fabric Connect documents: <ul style="list-style-type: none"> • <i>Configuring Fabric Basics and Layer 2 Services</i> • <i>Configuring Fabric Layer 3 Services</i> • <i>Configuring Fabric Multicast Services</i> 	6.1
Fabric Extend For more information, see <i>Configuring Fabric Basics and Layer 2 Services</i> .	n/a
Fabric RSPAN (Mirror to I-SID) For more information, see <i>Troubleshooting</i> .	n/a
File Transfer Protocol (FTP) server and client (IPv4) For more information, see <i>Administering</i> .	4.5
File Transfer Protocol (FTP) server and client (IPv6) For more information, see <i>Administering</i> .	6.2

Table continues...

Feature	Release
First Hop Security (FHS) For more information, see <i>Configuring Security</i> .	n/a
FHS - DHCPv6 Guard	n/a
FHS - DHCP Snooping (IPv4)	n/a
FHS - DHCP Snooping (IPv6)	n/a
FHS - IP Source Guard (IPv4 and IPv6)	n/a
FHS - Neighbor Discovery Inspection (IPv6)	n/a
FHS - IPv6 Router Advertisement (RA) Guard	n/a
Flight Recorder for system health monitoring For more information, see <i>Troubleshooting</i> .	4.5
Forgiving mode for CWDM and DWDM SFP+ transceivers For more information, see Extreme Networks Pluggable Transceivers Installation Guide .	4.5
Gratuitous ARP filtering For more information, see <i>Configuring IPv4 Routing</i> .	4.5
High Availability CPU for a standalone switch For more information, see <i>Administering</i> .	4.5
High Availability CPU for Simplified vIST	6.2 (Demo mode only)
IEEE 802.1AG Connectivity Fault Management (CFM): <ul style="list-style-type: none"> • Layer 2 Ping • TraceRoute • TraceTree For more information, see <i>Configuring Fabric Basics and Layer 2 Services</i> .	4.5
IEEE 802.3X Pause frame transmit For more information, see <i>Administering</i> .	n/a
Industry Standard Discovery Protocol (ISDP) (CDP compatible) For more information, see <i>Administering</i> .	n/a
Ingress dual rate port policers For more information, see <i>Configuring QoS and ACL-Based Traffic Filtering</i> .	4.5
Internal BPG (IBGP)	4.5

Table continues...

Related Information

Feature	Release
For more information, see <i>Configuring BGP Services</i> .	
Internet Control Message Protocol (ICMP) For more information, see <i>Configuring IPv4 Routing</i> .	4.5
ICMP broadcast and multicast enable or disable For more information, see <i>Configuring IPv4 Routing and Configuring IPv6 Routing</i> .	4.5
Internet Group Management Protocol (IGMP), including virtualization For more information, see <i>Configuring IP Multicast Routing Protocols</i> .	4.5
Internet Key Exchange (IKE) v2 For more information, see <i>Configuring Security</i> .	n/a
Inter-VSN routing For more information, see <i>Configuring Fabric Layer 3 Services</i> .	6.1
IP Multicast over Fabric Connect For more information, see <i>Configuring Fabric Multicast Services</i> .	6.2
IP route policies For more information, see <i>Configuring IPv4 Routing</i> .	4.5
IP Shortcut routing including ECMP For more information, see <i>Configuring Fabric Layer 3 Services</i> .	6.1
IP Source Guard (IPv4 and IPv6) For more information, see <i>Configuring Security</i> .	n/a
IP Source Routing enable or disable For more information, see <i>Configuring IPv4 Routing and Configuring IPv6 Routing</i> .	4.5
IPsec for IPv6 For more information, see <i>Configuring Security</i> .	n/a
IPv6 (OSPFv3, VRRP, RSMLT, DHCP Relay, IPv4 in IPv6 tunnels) For more information, see <i>Configuring IPv6 Routing</i> .	6.2
IPv6 ACL filters For more information, see <i>Configuring QoS and ACL-Based Traffic Filtering</i> .	6.2 (on Ingress only)

Table continues...

Feature	Release
IPv6 inter-VSN routing For more information, see <i>Configuring Fabric Layer 3 Services</i> .	n/a
IPv6 mode flag (<code>boot config flags ipv6-mode</code>) For more information, see <i>Configuring IPv6 Routing</i> .	n/a
IPv6 Shortcut routing For more information, see <i>Configuring Fabric Layer 3 Services</i> .	n/a
IPv6 Virtualization for the following features and functions: <ul style="list-style-type: none"> • IPv6 Interfaces and IPv6 Static Routes in VRFs and Layer 3 VSNs • ECMP and Alternative route • VRRPv3 for IPv6 • DHCP Relay • IPv6 Reverse Path Forwarding • ICMP Ping and Traceroute For more information, see <i>Configuring IPv6 Routing</i> .	n/a
IS-IS accept policies For more information, see <i>Configuring Fabric Layer 3 Services</i> .	6.1
IS-IS authentication with SHA-256 For more information, see <i>Configuring Fabric Basics and Layer 2 Services</i> .	6.1
Key Health Indicator (KHI) For more information, see <i>Monitoring Performance</i> .	4.5
Layer 2 Video Surveillance install script For more information, see <i>Configuring Fabric Basics and Layer 2 Services</i> .	n/a
Layer 3 Video Surveillance install script (formerly known as the run vms endura script) For more information, see <i>Configuring Fabric Layer 3 Services</i> .	n/a
Layer 2 Virtual Service Network (VSN) For more information, see <i>Configuring Fabric Basics and Layer 2 Services</i> .	4.5

Table continues...

Related Information

Feature	Release
Layer 3 switch cluster (Routed SMLT) with Simplified vIST For more information, see <i>Configuring Link Aggregation, MLT, SMLT, and vIST</i> .	4.5
Layer 3 switch cluster (Routed SMLT) with Virtual Inter-Switch Trunk (vIST) For more information, see <i>Configuring Link Aggregation, MLT, SMLT, and vIST</i> .	6.1
Layer 3 VSN For more information, see <i>Configuring Fabric Layer 3 Services</i> .	6.1
linerate-directed-broadcast boot flag (boot config flags linerate-directed-broadcast) For more information, see <i>Administering</i> .	n/a
Link Layer Discovery Protocol (LLDP) For more information, see <i>Administering</i> .	6.1
Logging to a file and syslog (IPv4) For more information, see <i>Monitoring Performance</i> .	4.5
Logging to a file and syslog (IPv6) For more information, see <i>Monitoring Performance</i> .	6.2
Logon banner For more information, see <i>Administering</i> .	n/a
MAC security (MAC-layer filtering, limit learning) For more information, see <i>Configuring VLANs, Spanning Tree, and NLB</i> .	n/a
MACsec 2AN mode For more information, see <i>Configuring Security</i> .	n/a
MACsec 4AN mode For more information, see <i>Configuring Security</i> .	4.5
Mirroring (port and flow-based) For more information, see <i>Troubleshooting</i> .	4.5
Multicast Listener Discovery (MLD) For more information, see <i>Configuring IP Multicast Routing Protocols</i> .	n/a
Multicast route (mroute) statistics for IPv4 and IPv6	n/a

Table continues...

Feature	Release
For more information, see <i>Configuring IP Multicast Routing Protocols</i> .	
MultiLink Trunking (MLT) / Link Aggregation Group (LAG) For more information, see <i>Configuring Link Aggregation, MLT, SMLT, and vIST</i> .	4.5
Neighbor Discovery Inspection (IPv6) For more information, see <i>Configuring Security</i> .	n/a
Network Load Balancing (NLB) - multicast operation For more information, see <i>Configuring VLANs, Spanning Tree, and NLB</i> .	n/a
Network Load Balancing (NLB) - unicast operation For more information, see <i>Configuring VLANs, Spanning Tree, and NLB</i> .	4.5
Network Time Protocol version 3 (NTPv3) For more information, see <i>Administering</i> .	4.5
nmi-mstp boot flag (<code>boot config flags nmi-mstp</code>) ! Important: This flag has special upgrade considerations the first time you upgrade to a release that supports it. For more information, see <i>Administering</i> .	n/a
Non EAPoL MAC RADIUS authentication For more information, see <i>Configuring Security</i> .	n/a
Open Shortest Path First (OSPF) For more information, see <i>Configuring OSPF and RIP</i> .	4.5
P-Bridge MIB Adds support for: <ul style="list-style-type: none"> • dot1dExtBase Group • dot1dDeviceCapabilities • dot1dTrafficClassesEnabled • dot1dGmrpStatus • dot1dPortCapabilitiesTable 	6.1

Table continues...

Related Information

Feature	Release
Protocol Independent Multicast-Sparse Mode (PIM-SM), PIM-Source Specific Mode (PIM-SSM) for IPv4 For more information, see <i>Configuring IP Multicast Routing Protocols</i> .	4.5
PIM and PIM-SSM over IPv6 For more information, see <i>Configuring IP Multicast Routing Protocols</i> .	n/a
Power Management For more information, see <i>Administering</i> .	n/a
Power over Ethernet (PoE) For more information, see <i>Administering</i> .	n/a
PoE/PoE+ allocation using LLDP For more information, see <i>Administering</i> .	n/a
QoS Access Control Entries (ACE) For more information, see <i>Configuring QoS and ACL-Based Traffic Filtering</i> .	6.2
QoS ingress port rate limiter For more information, see <i>Configuring QoS and ACL-Based Traffic Filtering</i> .	n/a
RADIUS (IPv6) For more information, see <i>Configuring Security</i> .	6.2
RADIUS, community-based users (IPv4) For more information, see <i>Configuring Security</i> .	4.5
RADIUS secure communication using IPSec for IPv4 For more information, see <i>Configuring Security</i> .	n/a
RADIUS secure communication using IPSec for IPv6 For more information, see <i>Configuring Security</i> .	n/a
Remote Login (Rlogin) server/client (IPv4) For more information, see <i>Administering</i> .	4.5
Rlogin server (IPv6) For more information, see <i>Administering</i> .	6.2
Remote Monitoring 1 (RMON1) for Layer 1 and Layer 2 For more information, see <i>Monitoring Performance</i> .	4.5
Remote Monitoring 2 (RMON2) for network and application layer protocols	n/a

Table continues...


Feature	Release
For more information, see <i>Monitoring Performance</i> .	
Remote Shell (RSH) server/client For more information, see <i>Administering</i> .	4.5
Route Information Protocol (RIP) For more information, see <i>Configuring OSPF and RIP</i> .	4.5
RIPng For more information, see <i>Configuring IPv6 Routing</i> .	6.2
run spbm installation script For more information, see <i>Configuring Fabric Basics and Layer 2 Services</i> .	n/a
Secure Copy (SCP)  Note: The switch does not support the WinSCP client. For more information, see <i>Administering</i> .	4.5
Secure hash algorithm 1 (SHA-1) and SHA-2 For more information, see <i>Configuring OSPF and RIP</i> .	4.5
Secure Shell (SSH) (IPv4) For more information, see <i>Administering</i> .	4.5
Secure Sockets Layer (SSL) certificate management For more information, see <i>Administering</i> .	4.5
Security ACEs For more information, see <i>Configuring QoS and ACL-Based Traffic Filtering</i> .	4.5
sFlow For more information, see <i>Monitoring Performance</i> .	6.2
sFlow collector reachability on user-created VRFs For more information, see <i>Monitoring Performance</i> .	6.2
Simple Loop Prevention Protocol (SLPP) For more information, see <i>Configuring VLANs, Spanning Tree, and NLB</i> .	4.5
Simple Mail Transfer Protocol (SMTP) for log notification For more information, see <i>Monitoring Performance</i> .	6.1

Table continues...

Related Information

Feature	Release
Simple Network Management Protocol (SNMP) v1/2/3 (IPv4) For more information, see <i>Configuring Security</i> .	4.5
SLA Mon For more information, see <i>Configuring the SLA Mon Agent</i> .	4.5
SLPP Guard For more information, see <i>Configuring Link Aggregation, MLT, SMLT, and vIST</i> .	6.2
SNMP (IPv6) For more information, see <i>Configuring Security</i> .	6.2
SoNMP For more information, see <i>Administering</i> .	4.5
Spanning Tree Protocol (STP): <ul style="list-style-type: none"> • Multiple STP (MSTP) • Rapid STP (RSTP) For more information, see <i>Configuring VLANs, Spanning Tree, and NLB</i> .	4.5
spbm-config-mode (<code>boot config flags spbm-config-mode</code>) For more information, see <i>Configuring IP Multicast Routing Protocols</i> .	4.5
SPB-PIM Gateway controller node For more information see <i>Configuring Fabric Multicast Services</i> .	n/a
SPB-PIM Gateway interface For more information see <i>Configuring Fabric Multicast Services</i> .	n/a
SSH (IPv6) For more information, see <i>Administering</i> .	6.2
SSH client disable For more information, see <i>Administering</i> .	4.5
SSH key size For more information, see <i>Administering</i> .	6.1
SSH rekey For more information, see <i>Administering</i> .	6.1

Table continues...

Feature	Release
Static routing For more information, see <i>Configuring IPv4 Routing</i> .	4.5
Suspend duplicate system ID detection For more information, see <i>Configuring Fabric Basics and Layer 2 Services</i> .	6.1
Switch cluster (multi-chassis LAG) -Virtual Inter-Switch Trunk (vIST) For more information, see <i>Configuring Link Aggregation, MLT, SMLT, and vIST</i> .	6.1
Switched UNI For more information, see <i>Configuring Fabric Basics and Layer 2 Services</i> .	n/a
TACACS+ For more information, see <i>Configuring Security</i> .	4.5
TACACS+ secure communication using IPSec for IPv4 For more information, see <i>Configuring Security</i> .	n/a
Telnet server and client (IPv4) For more information, see <i>Administering</i> .	4.5
Telnet server and client (IPv6) For more information, see <i>Administering</i> .	6.2
TLS server for secure HTTPS For more information, see <i>Configuring User Interfaces and Operating Systems</i> .	6.1
TLS client for secure syslog For more information, see <i>Troubleshooting</i> .	n/a
Transparent Port UNI (T-UNI) For more information, see <i>Configuring Fabric Basics and Layer 2 Services</i> .	n/a
Trivial File Transfer Protocol (TFTP) server and client (IPv4) For more information, see <i>Administering</i> .	4.5
TFTP server and client (IPv6) For more information, see <i>Administering</i> .	6.2
Unicast Reverse Path Forwarding (URPF) checking (IPv4 and IPv6)	4.5

Table continues...

Feature	Release
<p>Note: Supported on IPv4 only. For more information, see <i>Configuring Security</i>.</p>	
<p>Virtual Inter-Switch Trunk (vIST) For more information, see <i>Configuring Link Aggregation, MLT, SMLT, and vIST</i>.</p>	6.1
<p>Virtual Link Aggregation Control Protocol (VLACP) For more information, see <i>Configuring Link Aggregation, MLT, SMLT, and vIST</i>.</p>	4.5
<p>Virtual Router Redundancy Protocol (VRRP) For more information, see <i>Configuring IPv4 Routing</i>.</p>	4.5
<p>Virtualization with IPv4 Virtual Routing and Forwarding (VRF)</p> <ul style="list-style-type: none"> • ARP • DHCP Relay • Inter-VRF Routing (static, dynamic, and policy) • Local routing • OSPFv2 • RIPv1 and v2 • Route policies • Static routing • VRRP <p>For more information, see <i>Configuring IPv4 Routing</i>.</p>	4.5
<p>Increased VRF and Layer 3 scaling (The VSP 8600 automatically supports the maximum number of VRFs without additional VLAN reservation.) For more information, see <i>Configuring IPv4 Routing</i>.</p>	n/a
<p>VRRPv3 for IPv4 and IPv6 For more information, see <i>Configuring IPv4 Routing and Configuring IPv6 Routing</i>.</p>	6.1
<p>VXLAN Gateway For more information, see <i>Configuring VLANs, Spanning Tree, and NLB</i>.</p>	n/a

New MIBs

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

Object Name	Object OID
rcAppTelemetry	1.3.6.1.4.1.2272.1.226
rcAppTelemetryMib	1.3.6.1.4.1.2272.1.226.1
rcAppTelemetryNotifications	1.3.6.1.4.1.2272.1.226.1.1
rcAppTelemetryObjects	1.3.6.1.4.1.2272.1.226.1.2
rcAppTelemetryScalars	1.3.6.1.4.1.2272.1.226.1.2.1
rcAppTelemetryAdminEnable	1.3.6.1.4.1.2272.1.226.1.2.1.1
rcAppTelemetryClearCounterStats	1.3.6.1.4.1.2272.1.226.1.2.1.2
rcAppTelemetryCounterTable	1.3.6.1.4.1.2272.1.226.1.2.2
rcAppTelemetryCounterEntry	1.3.6.1.4.1.2272.1.226.1.2.2.1
rcAppTelemetryCounterId	1.3.6.1.4.1.2272.1.226.1.2.2.1.1
rcAppTelemetryCounterName	1.3.6.1.4.1.2272.1.226.1.2.2.1.2
rcAppTelemetryCounterPkts	1.3.6.1.4.1.2272.1.226.1.2.2.1.3
rcAppTelemetryCounterBytes	1.3.6.1.4.1.2272.1.226.1.2.2.1.4
rcAppTelemetryCounterClearCounter	1.3.6.1.4.1.2272.1.226.1.2.2.1.5
rcSflow	1.3.6.1.4.1.2272.1.221
rcSflowMib	1.3.6.1.4.1.2272.1.221.1
rcSflowObjects	1.3.6.1.4.1.2272.1.221.1.1
rcSflowScalars	1.3.6.1.4.1.2272.1.221.1.1.1
rcSflowAdminEnable	1.3.6.1.4.1.2272.1.221.1.1.1.1
rcSflowAgentAddressType	1.3.6.1.4.1.2272.1.221.1.1.1.2
rcSflowAgentAddress	1.3.6.1.4.1.2272.1.221.1.1.1.3
rcSflowStatsTable	1.3.6.1.4.1.2272.1.221.1.1.2
rcSflowStatsEntry	1.3.6.1.4.1.2272.1.221.1.1.2.1
rcSflowStatsIndex	1.3.6.1.4.1.2272.1.221.1.1.2.1.1
rcSflowStatsDatagramCount	1.3.6.1.4.1.2272.1.221.1.1.2.1.2
rcSflowStatsClearStats	1.3.6.1.4.1.2272.1.221.1.1.2.1.3
rcSflowExtRcvrTable	1.3.6.1.4.1.2272.1.221.1.1.3
rcSflowExtRcvrEntry	1.3.6.1.4.1.2272.1.221.1.1.3.1
rcSflowExtRcvrVrfName	1.3.6.1.4.1.2272.1.221.1.1.3.1.1
sflow	1.3.6.1.4.1.14706
sFlowMIB	1.3.6.1.4.1.14706.1
sFlowAgent	1.3.6.1.4.1.14706.1.1

Table continues...

Related Information

Object Name	Object OID
sFlowRcvrTable	1.3.6.1.4.1.14706.1.1.4
sFlowRcvrEntry	1.3.6.1.4.1.14706.1.1.4.1
sFlowRcvrIndex	1.3.6.1.4.1.14706.1.1.4.1.1
sFlowRcvrOwner	1.3.6.1.4.1.14706.1.1.4.1.2
sFlowRcvrTimeout	1.3.6.1.4.1.14706.1.1.4.1.3
sFlowRcvrMaximumDatagramSize	1.3.6.1.4.1.14706.1.1.4.1.4
sFlowRcvrAddressType	1.3.6.1.4.1.14706.1.1.4.1.5
sFlowRcvrAddress	1.3.6.1.4.1.14706.1.1.4.1.6
sFlowRcvrPort	1.3.6.1.4.1.14706.1.1.4.1.7
sFlowRcvrDatagramVersion	1.3.6.1.4.1.14706.1.1.4.1.8
sFlowFsTable	1.3.6.1.4.1.14706.1.1.5
sFlowFsEntry	1.3.6.1.4.1.14706.1.1.5.1
sFlowFsDataSource	1.3.6.1.4.1.14706.1.1.5.1.1
sFlowFsInstance	1.3.6.1.4.1.14706.1.1.5.1.2
sFlowFsReceiver	1.3.6.1.4.1.14706.1.1.5.1.3
sFlowFsPacketSamplingRate	1.3.6.1.4.1.14706.1.1.5.1.4
sFlowFsMaximumHeaderSize	1.3.6.1.4.1.14706.1.1.5.1.5
sFlowCpTable	1.3.6.1.4.1.14706.1.1.6
sFlowCpEntry	1.3.6.1.4.1.14706.1.1.6.1
sFlowCpDataSource	1.3.6.1.4.1.14706.1.1.6.1.1
sFlowCpInstance	1.3.6.1.4.1.14706.1.1.6.1.2
sFlowCpReceiver	1.3.6.1.4.1.14706.1.1.6.1.3
sFlowCpInterval	1.3.6.1.4.1.14706.1.1.6.1.4
rcPrFilterAceId	1.3.6.1.4.1.2272.1.202.1.1.2.4.1.1.2
rcPrFilterAceRemarkDscp	1.3.6.1.4.1.2272.1.202.1.1.2.4.1.1.5
rcPrFilterAceInternalQos	1.3.6.1.4.1.2272.1.202.1.1.2.4.1.1.25