Extreme networks

VSP 8600 Release Notes

For VSP 8600 Release 8.1

9037143-00 Rev AC
December 2023

Legal Notice

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

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

Trademarks

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

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

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

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

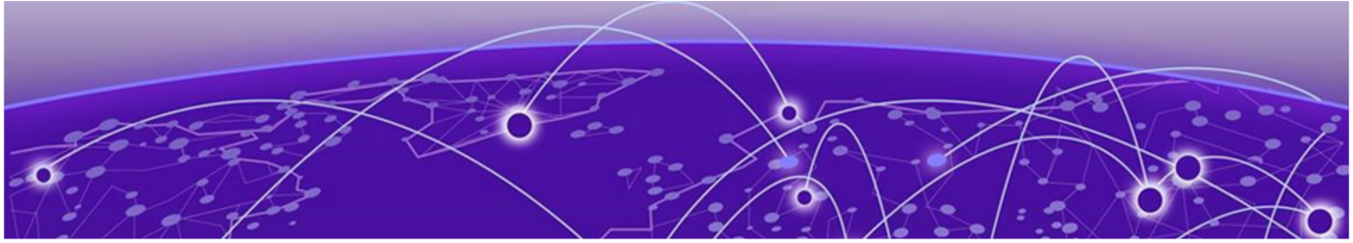
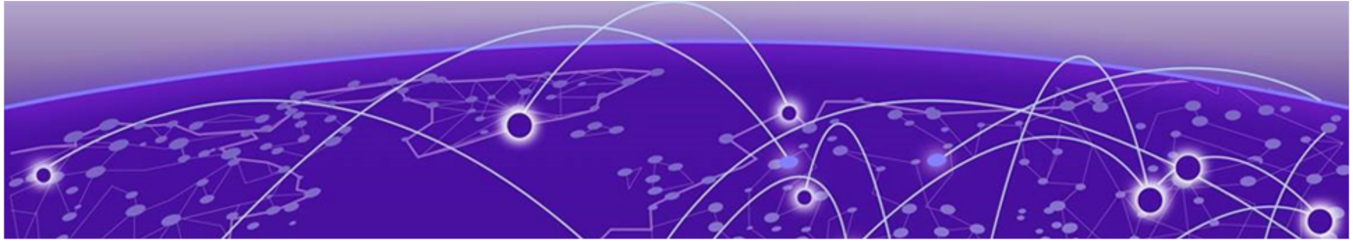


Table of Contents



About this Document

The topics in this section discuss the purpose of this document, the conventions used, ways to provide feedback, additional help, and information regarding other Extreme Networks publications.

Purpose

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

This document includes the following information:

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

Conventions

To help you better understand the information presented in this guide, the following topics describe the formatting conventions used for notes, text, and other elements.

Text Conventions

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

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
💡	Tip	Helpful tips and notices for using the product.
📝	Note	Useful information or instructions.
➡	Important	Important features or instructions.
⚠	Caution	Risk of personal injury, system damage, or loss of data.
⚠	Warning	Risk of severe personal injury.

Table 2: Text Conventions

Convention	Description
Angle brackets (< >)	Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. If the command syntax is `cfm maintenance-domain maintenance-level <0-7>` , you can enter `cfm maintenance-domain maintenance-level 4`.
Bold text	Bold text indicates the GUI object name you must act upon. Examples: • Click **OK**. • On the **Tools** menu, choose **Options**.
Braces ({ })	Braces ({ }) indicate required elements in syntax descriptions. Do not type the braces when you enter the command. For example, if the command syntax is `ip address {A.B.C.D}`, you must enter the IP address in dotted, decimal notation.

Table 2: Text Conventions (continued)

Convention	Description
Brackets ([ ])	Brackets ([ ]) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command. For example, if the command syntax is `show clock [detail]`, you can enter either `show clock` or `show clock detail`.
Ellipses (…)	An ellipsis (…) indicates that you repeat the last element of the command as needed. For example, if the command syntax is `ethernet/2/1 [ <parameter> <value> ]...`, you enter `ethernet/2/1` and as many parameter-value pairs as you need.
Italic Text	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.
`Plain Courier Text`	Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages. Examples: • `show ip route` • `Error: Invalid command syntax [Failed][2013-03-22 13:37:03.303 -04:00]`
Separator (>)	A greater than sign (>) shows separation in menu paths. For example, in the Navigation tree, expand the **Configuration** > **Edit** folders.
Vertical Line (|)	A vertical line (|) separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command. For example, if the command syntax is `access-policy by-mac action { allow | deny }`, you enter either `access-policy by-mac action allow` or `access-policy by-mac action deny`, but not both.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation

Release Notes

Hardware and Software Compatibility for Extreme Networks products

Extreme Optics Compatibility

Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

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

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

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

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)

- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

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

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

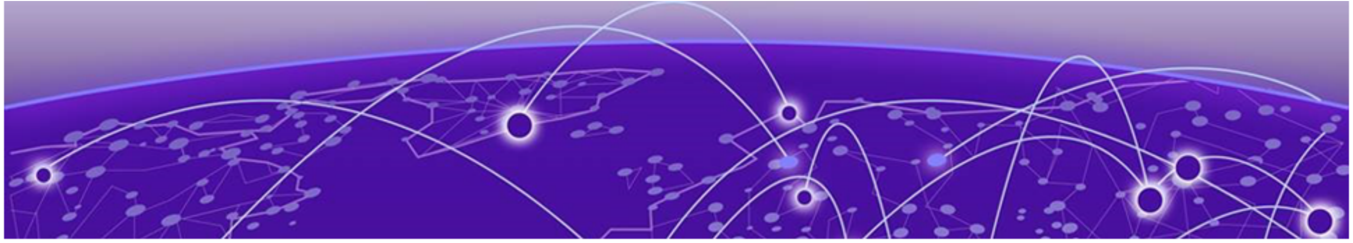
Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

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

To send feedback, email us at documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



New in this Release

The following sections detail what is new in VSP 8600 Series Release 8.1.

New Transceivers and Components

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

- 100 Gb transceiver modules
  - 100G FR QSFP28 2km LC connector Single-Mode MSA (PN: 100G-FR-QSFP2KM)
  - 100G SR4 QSFP28 100m MPO connector Multi-Mode MSA (PN: 100G-SR4-QSFP100M)
- 25 Gb cables
  - 25G Passive DAC SFP28 Copper Cable 0.5m MSA (PN: 25G-DACP-SFPZ5M), 0.5 meter

Note
25 Gb transceiver module use on VSP 8600 Series requires the 100G QSFP28 SFP28 adapter (PN: 10506) and channelization enabled on a 100 Gb port.

Extreme Networks can announce support for additional optical components in the future. Check the following documents for a complete and current list of supported optical components:

Compatibility for Extreme Networks SFP, SFP+, SFP28, QSFP+, and QSFP28 transceiver modules with the VSP Series switches	Extreme Optics website
Descriptions of Extreme Networks optical transceivers and components	Extreme Optics website

Auto-sense NNI LLDP Signaling for Zero-Touch Fabric Connect

This release implements support for the Link Layer Discovery Protocol (LLDP) Fabric Connect Type–Length–Value (TLV) on the VSP 8600 Series. The LLDP Fabric Connect

TLV contains details about the pre-configured B-VLANs and system ID that a system sends to other devices in a network topology.

For more information, see *VOSS User Guide*.

Factorydefaults Flag Behavior Enhancements

The factorydefaults boot flag now removes the runtime, primary, and backup configuration files, resets all local default user account passwords, and removes all digital certificates. The Radsec, IPsec, IKE, OSPF, SNMP, SSL, SSH, OVSDB, and NTP files are also removed. The CLI displays a warning that the configurations, passwords, and files will be reset, and the system logs an informational message. The configuration and file removals occur during the next boot sequence when the factorydefaults boot flag is enabled. After the switch reboots, the security mode setting is retained. To enable Zero Touch Onboarding after a factorydefaults boot, reboot the switch again without saving a configuration.

For more information, see *VOSS User Guide*.

Force User to Change Default Password on First Login

In previous releases, you could use a default password to initially access the CLI. Now a password change is required to access the CLI on first login after a factory default or if your switch has no primary or backup configuration files. The system provides three attempts to change the password. If unsuccessful, you are taken back to the login prompt but you are not locked out. You cannot use an empty password. A password change is required irrespective of security mode, console, SSH, or Telnet access.

For more information, see *VOSS User Guide*.

IPv6 OSPFv3 Neighbor Advertisements without R-bit

This release introduces OSPFv3 neighbor advertisements without R-bit. If an OSPFv3 neighbor does not provide the R-bit in the Network Discovery (ND) packet, the system enables R-bit for every OSPFv3 neighbor with dependent routes to avoid deletion resulting from inactivity. An OSPFv3 neighbor without R-bit that experiences a timeout can now trigger the Network Unreachability Detection (NUD), instead of being deleted.

For more information, see *VOSS User Guide*.

IPv6 OSPFv3 on CLIP Interfaces

This release adds support for Open Shortest Path First Version 3 (OSPFv3) configuration on circuitless IP (CLIP) interfaces for the Global Router or a specific Virtual Router Forwarding (VRF) instance. The switch supports a maximum of 64 OSPFv3 CLIP interfaces.

For more information, see *VOSS User Guide*.

Key Health Indicator Enhancements

This release adds a Key Health Indicator (KHI) new parameter `rx-queue` to the command **`show khi performance`** to display the queue performance and utilization statistics on the switch.

For more information, see *VOSS User Guide*.

Log Earlier Warning Messages for FDB Table Scaling Limits

The log now shows warning messages earlier when approaching FDB scaling limits. When reaching 75% and higher of FDB table scaling limit, the system begins logging warning messages so you can take corrective action while the node remains responsive. You can contact support before the limit is reached to troubleshoot the cause of the increase.

For more information, see *VOSS User Guide*.

MACsec Key Agreement on VSP 8600 Series

MACsec Key Agreement (MKA) protocol discovers mutually authenticated MACsec peers, and elects one as a key server. The key server generates and distributes Secure Association Keys (SAKs), which are used at both ends of an Ethernet link to encrypt and decrypt frames. The key server periodically generates and distributes SAKs to maintain the link for as long as MACsec is enabled.

This release adds support for MKA on VSP 8600 Series switches.

For more information, see *VOSS User Guide*.

MACsec on 8606CQ IOC Module Channelized Ports

MACsec is now supported for channelized ports on an 8606CQ IOC module. MACsec is supported on 8606CQ channelized ports in 4x10 Gbps or 4x25 Gbps configurations. If you enable channelization on a port, the MACsec configuration migrates from the main port to the first subport. If you disable channelization on a port, the MACsec configuration migrates from the first subport to the main port.

For more information, see *VOSS User Guide*.

New Features with High Availability-CPU (HA-CPU) Support

The following new features have HA-CPU support:

> **Note**
>
> All IPv6 applications have partial HA-CPU support. The system synchronizes user configuration data, including IPv6 addresses and static routes from the primary CPU to the standby CPU. The system does not synchonize dynamic data from protocol learning. After a CPU failover, the IPv6 applications must restart and rebuild data tables, which causes an interruption of traffic that is dependent on the IPv6 protocol or applications with partial HA support.

- Factory Default flag behavior enhancements
- SHA512 secure password hashing
- MACsec Key Agreement (MKA)
- IPv6 OSPFv3 neighbor advertisements without R-bit
- IPv6 OSPFv3 support on circuitless IP interfaces

For more information, see *VOSS User Guide*.

NTP Authentication Key Obfuscation

In earlier releases, the secret key displayed in clear text on the console and in the configuration file when you assigned an authentication key to the server using the **`ntp server`** command.

In this release, the secret key is encrypted and is not visible on the console or in the configuration file. Asterisks now display as the secret key. The **`show ntp key`** CLI command output no longer displays the secret key field. The **keysecret** field in EDM is also removed.

For more information, see *VOSS User Guide*.

SHA512 Password Hashing

SHA2 512-bit password hashing is available as a security enhancement beyond the previous default SHA1 160-bit password hashing method. The new CLI command **`password hash`** is introduced to change the password hash between SHA1 and SHA2. The new default is SHA2 for new switches running this release.

If you change the password hash level, the system deletes all custom users and old password files. After a password hash level change, on first login each default user must change their password. If hsecure mode is enabled, a user password history is saved.

You can view the currently configured password hash level with the command **show cli password** or **show running-config module cli**.

Note

Switches upgraded to this release retain SHA1 password hashes and custom users, until a factory default reset or until the password hash level is changed. During a factory default reset, SHA2 512-bit becomes the default password hash, all custom users are deleted, and SHA1 passwords are removed.

In the case of a software downgrade to a release before VSP 8600 Series Release 8.1, all SHA2 password hashes roll back to SHA1 hashes with default passwords.

For more information, see *VOSS User Guide*.

Show IO Resources Enhancement

You can now view IO resources related debug information with the new parameters *l3-kaps-count*, *l3-lem-count*, and *model-dnx-stats* for the CLI command **show io resources**.

For more information, see *VOSS Command Line Interface Commands Reference*.

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 *VOSS User Guide*.

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

Table 3: Software Filenames and Sizes

Description	VSP 8600 Series	File size
SHA512 Checksum files	VOSS8600.8.1.0.0.sha512	1249 bytes
MD5 Checksum files	VOSS8600.8.1.0.0.md5	426 bytes
MIB - supported object names	VOSS8600.8.1.0.0_mib_sup.txt	1,159,472 bytes
MIB - zip file of all MIBs	VOSS8600.8.1.0.0_mib.zip	1,155,767 bytes
MIB - objects in the OID compile order	VOSS8600.8.1.0.0_mib.txt	7,662,193 bytes
EDM Help files	VOSS86v810_HELP_EDM_gzip.zip	5,127,813 bytes
Logs reference	VOSS8600.8.1.0.0_edoc.tar	66,119,360 bytes
Software image	VOSS8600.8.1.0.0.tgz	184,230,422 bytes

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

Table 4: Open Source Software Files

Copyright file
VOSS8600.8.1.0.0_oss-notice.html 2,766,227 bytes

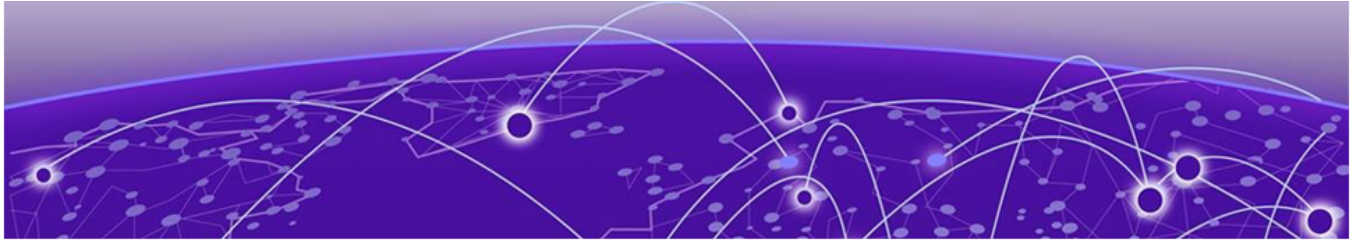
The Open Source license text for the switch is included on the product. You can access it by entering the following command in the CLI:

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

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

Documentation Changes

The Features by Release table has been removed from this document. Product support information for features is now described in product support tables at the beginning of each feature description throughout the documentation suite, and in the *VOSS Feature Support Matrix*.



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, 6.1, 6.2, 6.3 or 8.0 to VSP 8600 Series 8.1.

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

Upgrade Considerations

The 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 before you begin an image upgrade.

Note
If your switch is configured in High Availability Hot Standby mode with SNMPv3 users using SHA, you must change to Warm Standby mode before upgrading to this release. For more information, see Known Issues and Restrictions on page 32.

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.

IS-IS Authentication

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

Note

This applies only when you downgrade the software from the current release to 6.1.x.

It does not apply when you downgrade the software to 6.2.x.

Use the following procedure as a workaround:

1. Disable IS-IS Authentication on 100 Gb ports on both peers.
2. Downgrade the software to the required release.
3. Re-enable IS-IS Authentication.

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 a supported release starting with Release 6.1.x. If, for example, one end is running 6.1.x and the other end is running a different release, 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.

Usernames and Passwords Revert to Default

When downgrading from the current release to release 8.0.x or older, all configured users reset to the default usernames and passwords, and all custom users are deleted.

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

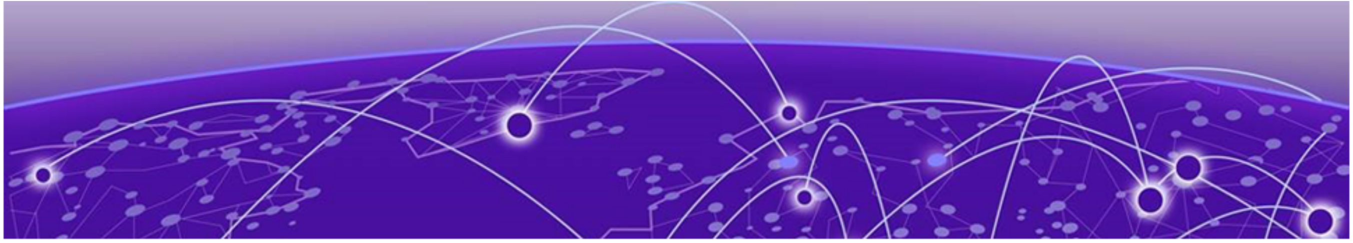
When there is a mismatch between the software running on the switch and the software on the IOC module, the switch updates the IOC module to the version of software running on the switch. During this process you see errors that are similar to the following:

```
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_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 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.

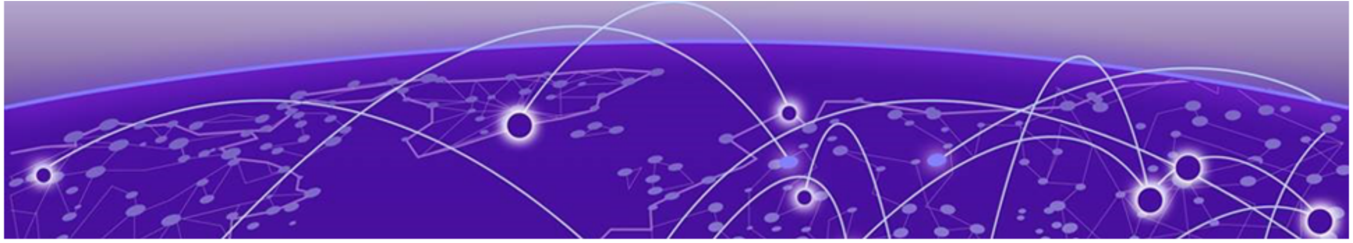
Note

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.



VSP 8600 Series Hardware and Software Compatibility

Part number	Model number	Initial software release	Supported new software release				
			6.1.0.0	6.2.0.0	6.3.0.0	8.0.0.0	8.1.0.0
EC8602001-E6	VSP 8608	4.5.0.0	Y	Y	Y	Y	Y
EC8602002-E6	VSP 8608 with 3 SF modules and 4 AC PSUs	4.5.0.0	Y	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	Y
EC8604001–E6	8600SF	4.5.0.0	Y	Y	Y	Y	Y
EC8604002-E6	8624XS	4.5.0.0	Y	Y	Y	Y	Y
EC8604003-E6	8624XT	4.5.0.0	Y	Y	Y	Y	Y
EC8604004-E6	8616QQ	4.5.0.0	Y	Y	Y	Y	Y
EC8604005-E6	8606CQ	4.5.0.1	Y	Y	Y	Y	Y



Software Scaling

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

Layer 2

Table 5: Layer 2 Maximums

Attribute	Maximum number supported
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
Switched UNI I-SIDs per switch (L2 only)	6000
Switched UNI endpoints per interface (same I-SID)	1

Table 5: Layer 2 Maximums (continued)

Attribute	Maximum number supported
Switched UNI endpoints per interface (different I-SIDs)	4000
Transparent Port UNI services per switch (port mapped to I-SID)	192
VLACP interfaces	128

IP Unicast

Table 6: IP Unicast Maximums

Attribute	Maximum number supported
BGP+ peers	16
DHCP Relay forwarding entries (IPv4 or IPv6)	512 per VRF/2,048 per switch
ECMP groups/paths per group	1,000/8
IP interfaces (IPv4 or IPv6 or IPv4+IPv6)	4,059*
* **NOTE:** The maximum limit for IP interfaces is 3,584, if the limit of 512 VRRP interfaces is reached.	
IPv4 ARP table	64,000
IPv4 BGP peers	256
IPv4 CLIP interfaces	64
IPv4 RIP interfaces	200
IPv4 route policies (per VRF/per switch)	500/5,000
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/IPv6 VRF instances	512*
Note: The maximum number of VRFs for inter-VRF redistribution is 256.	
IPv6 BGP Peers (GRT and all VRFs combined)	256
IPv6 CLIP interfaces	64
IPv6 Ingress ACEs (Security and QoS)	2,000
IPv6 Neighbor table	16,000
IPv6 OSPFv3 routes (GRT and VRFs combined)	32,000
IPv6 RIPng peers	48
IPv6 RIPng routes	16,000
IPv6 Route Table size	32,000

Table 6: IP Unicast Maximums (continued)

Attribute	Maximum number supported
IPv6 static neighbor records	128 per VRF or 1,000 per switch
IPv6 static routes	10,000
Layer 3 VSNs	512
Manually configured 6-in-4 tunnels	16
OSPF virtual instances	64
OSPF v2/v3 neighbors (GRT and all VRFs combined)	500
OSPFv2 areas	12 per VRF or GRT/80 per switch
OSPFv3 areas (GRT and VRFs combined)	64
OSPFv2/v3 interfaces (GRT and all VRFs, active/ passive)	500/2,000
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)

DvR

Table 7: DvR Maximums

Attribute	Maximum number supported
DvR domains per SPB fabric.	16
Controller nodes per DvR domain with default route inject flag enabled. Total number of Controllers per domain cannot exceed 8. Note: A DvR domain containing only Controller nodes and no Leaf nodes can have more than 8 Controllers per domain.	8
DvR host routes per DvR domain.	40,000

Layer 3 Route Table Size

Table 8: Layer 3 Route Table Size Maximums

Attribute	Maximum number supported
IPv4 BGP routes (control plane only)	1.5 M
IPv4 OSPF routes	64,000

Table 8: Layer 3 Route Table Size Maximums (continued)

Attribute		Maximum number supported
IPv4 RIP routes (per VRF/per switch)		2,000/16,000
IPv4 routes		252,000
IPv4 SPB Shortcut routes		16,000
IPv6 Shortcut routes (Incoming, processed ISIS routes):		32,000
IPv6 Shortcut routes (Outgoing, advertised ISIS routes):		
	64-bit long prefix	22,000
	128-bit long prefix	15,000
	prefix length 64-128 (across all VRFs)	16,000

IP Multicast

Table 9: IP Multicast Maximums

Attribute	Maximum number supported
IGMP interfaces	4,000
PIM interfaces (Active/Passive)	512/3,000
Multicast receivers/IGMP receiver entries (per switch)	6,000*
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.	
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 10: Filters, QoS, and Security Maximums

Attribute	Maximum number supported
Total ACE - Ingress	3,500 (2,000 IPv4 ACEs and 1,500 IPv6 ACEs)
Total ACE - Egress	2,000
Total ACL - Ingress	2,000
Total ACL - Egress	1,000

Fabric Scaling

Table 11: Fabric Scaling Maximums

Attribute	Maximum number supported
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.	
SPB multicast nodes per domain	1000
Multicast streams per BEB	6000
Multicast streams per BCB	15,000
Number of VLANs per FA enabled link	94
Maximum number of FA assignment mappings	4,500
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

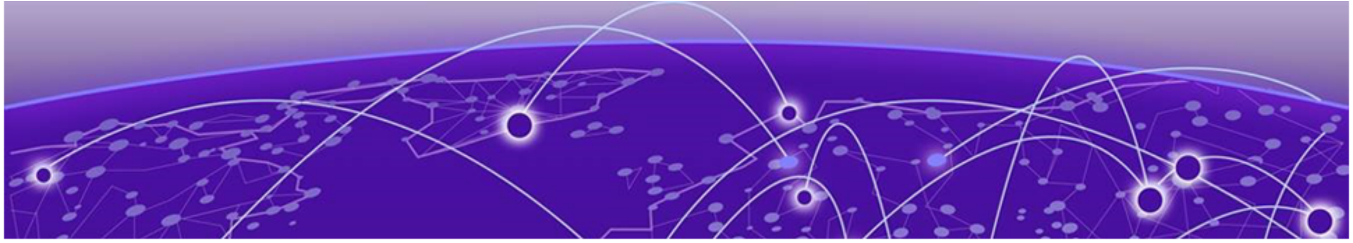
OAM and Diagnostics

Table 12: OAM and Diagnostics Maximums

Attribute	Maximum number supported
EDM sessions	5
FTP sessions	4

Table 12: OAM and Diagnostics Maximums (continued)

Attribute	Maximum number supported
Mirrored destination ports	4
Mirroring ports	191
Rlogin sessions	8
sFlow sampling rate	5000 samples per second per IOC module
SSH sessions	8
Telnet sessions	8



Important Notices

This section provides important information for this release.

Improved MAC Statistics Diagnostics

Use the command **show io control {slot[-slot][,...]}** to capture MAC address-movement statistics on a single slot, for improved diagnostics.

Example:

```
VSP8600:1#show io control

CP to SSIO MAC Statistics
Slot  Add      Delete   Refresh  Move
1     4168     24362    265886   0
2     4168     20207    0        0
4     4168     20184    0        0

HW to SSIO MAC statistics
Slot  Delete    Add       Report    Learn     Age       Move      Unsupported  Unknown
1     0         0         0         5724      4178      37        0
0
2     0         0         0         3637      2959      3110      0
0
4     0         0         0         174       2888      3633      0            0
```

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	Can test licensed features. The following types of Trial Licenses are available: • allows the use of all features excluding MACsec • allows the use of all features including MACsec Note: You can activate a Trial License once per switch.

Offer Level	Period	Support
IOC Base License		Can use Base software features on the switch. 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.
Feature Pack		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. Feature Pack licenses that the VSP 8600 supports: Layer 3 Virtualization: • Layer 3 Virtual Services Networks (VSNs) • DvR Controller • Greater than 25 VRFs • Greater than 17 BGP Peers Layer 3 Virtualization with MACsec: • Layer 3 Virtual Services Networks (VSNs) • DvR Controller • Greater than 25 VRFs • Greater than 17 BGP Peers • MACsec

For more information about licenses, see *VOSS User Guide*.

Limitations on license filename size

When you dynamically load a named license file, ensure that the file name has a maximum of 42 characters *including* the .xml extension. In other words, the length of the file name must be less than or equal to 42 characters, including the extension.

Otherwise, the license file does not load successfully on system reboot.

High Availability (HA)

VSP 8600 supports High Availability (HA) controller redundancy. Each IOC module supports both I/O and supervisor/controller functionality. An IOC inserted in Slot 1/2 acts as the Primary/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 Primary and Standby IOCs. In Warm Standby mode, if there is a software failure on the Primary 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 Primary and Standby, ensuring a hitless switchover upon Primary IOC failure.

Important
Hot Standby does not support configurations with SPBM or IPv6 features.

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
```

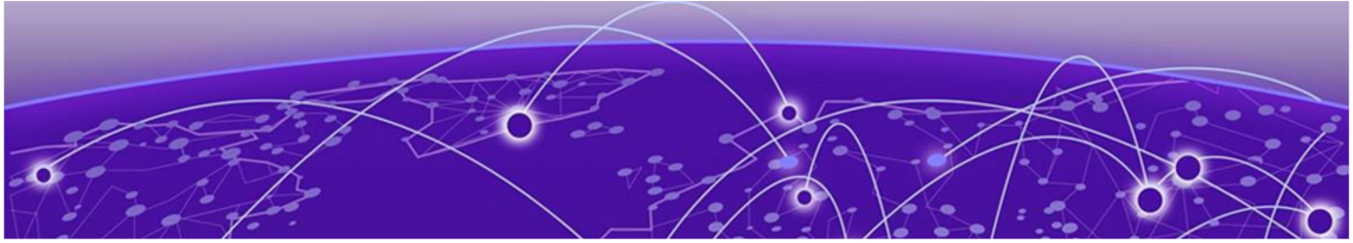
At this point you have used all the VRIDs in the selected range (2–9). Now you must start reusing the VRIDs from 2 to 9 for all other VRRP enabled VLANs. The following example shows what happens when you do not reuse a VRID from the selected range.

```
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
```



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-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	**`sys action`** reset counters command does not reset ISIS control packets.	Use `clear isis` command to reset stats.
VOSS-6103	**`sys action`** reset counters command does not reset ISIS int-counters.	Use `clear isis` command to reset stats.

Issue number	Description	Workaround
VOSS-6104	**`sys action`** reset counters command does not reset any ISIS system stats.	Use `clear isis` command to reset stats.
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-7500	COM+ does not display correct number of IP OSPF ECMP routes.	No workaround. COM+ is no longer supported.
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.

Issue number	Description	Workaround
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: `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 WARNING map_local_port_to_connectorPort: INVALID LOCAL PORT OF 10000000` The messages stop when 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.	No workaround, but there is no operational impact.
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-8278	EDM does not have a field to configure the RSA user key.	Use the CLI to configure the RSA user key.

Issue number	Description	Workaround
VOSS-8444 VOSS-8758	Disabling IS-IS incorrectly can cause unforeseen problems including traffic loss.	Use the following procedure to disable IS-IS on a switch: 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 can deplete virtual memory and cause the following warning: `VmSize of proc cbcp-main.x(4429) is 1867272KB, above 90% of available 1782579KB(index 0).`	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 a multicast BMAC DA, and also if the ISID carried in the packet is terminated on that fabric connect node.	No workaround.
VOSS-9977	Filter statistics do not increment if the incoming packet is marked for drop AND the filter has an action of mirror. For example: Packets might 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). 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).	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.
VOSS-9985	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. To avoid this potential traffic loss, avoid having both static and dynamic receivers on an IGMPv3 interface.	No workaround.

Issue number	Description	Workaround
VOSS-10091	After deleting an IPVPN, you might see the following error message: `ercdDeleteIpmcRecord:1734 ercdIpmcLookupAvlTree() failed SrcIp: 0x1b000093, DstIp: 0xe6290000 vlan_id 0xfff` This issue has no impact on the switch operation.	No workaround.
VOSS-10362	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.	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-10681	After deleting an L3VSN VLAN running IPMC traffic and then recreating it in the GRT (VRF 0), you might see OSAL backtrace messages such as the following: 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] cbcp-main.x(show_stackframe+0x1c) [0x1141c4f0] This issue has no impact on the switch operation.	No workaround.
VOSS-10839	The **`no mvpn enable`** and **`no ipvpn`** 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: • Increase the IS-IS hold down timer. • Remove the multicast streams or the multicast receivers in that VRF and then execute **`no mvpn enable`** or **`no ipvpn`**.

Issue number	Description	Workaround
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. 1. Configure VLAN xxx with **`ip spbmulticast enable`** 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 **`ip spbmulticast enable`** 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 occurs and traffic is hashed to B, there will be minimal traffic outage until B creates the distribution tree on the SPBM core. Important: Configure VLAN xxx with ip spbmulticast enable 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 occurs and traffic is hashed to B, there will be minimal traffic outage until B creates the distribution tree on the SPBM core.	Use one of the following workarounds: • Bounce IP Multicast over Fabric Connect on A's VLAN xxx. • Create VLAN xxx on A and B with no traffic running.
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-11414	When IS-IS routes are removed because the next hop is no longer present, you might 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.

Issue number	Description	Workaround
VOSS-12399	The system displays continuous LACP/ SMLT aggregation transition messages when you configure SMLT on the MLT interface, in a triangular SMLT setup that does not have vIST configured.	In a triangular SMLT setup, if the participant switches are edge switches, do not configure SMLT on the MLT interfaces.
VOSS-12520	An error is displayed on the output console when multicast traffic with source IP address 0.0.0.0 is sent.	Configure an explicit filter rule to drop the packets with source IP address 0.0.0.0.
VOSS-13265	When multiple slots on the switch chassis are powered on at the same time, it causes the cards to power on multiple times.	When using the CLI, power on one card at a time.
VOSS-14044	When you upload the license file on the switch, the filename length must not exceed 42 characters, including the .xml extension. Otherwise, the file does not load successfully upon system reboot.	Ensure that the length of the license filename is less than or equal to 42 characters, including the .xml extension.
VOSS-15017	When you reset the switch chassis, the IO card can sometimes crash and reboot with "out of memory" errors. However, after the reboot, the card operates normally.	No workaround, but there is no operational impact to the card.
VOSS-16056	On DvR Controllers, the output of the command **`show dvr members`** can show an incorrect SPB L1 cost. However, there is no functional impact since this value is not used on DvR Controllers. It is used only on DvR Leaf nodes.	On DvR Contollers, use the command **`show isis spbm unicast-fib`** to show the correct SPB L1 cost value.
VOSS-18510	Privileged EXEC Authentication does not function on secondary CP in HA warm-standby mode on VSP 8600 Series.	Privileged EXEC password authentication feature is only supported in HA hot-standby mode on VSP 8600 Series.
VOSS-18703	Some DvR host routes might be missed by the **`clear dvr host-entries`** command, in a scaled up network with traffic running from all the hosts.	You can bounce IS-IS or the DvR controllers to clear the missed DvR host routes.
VOSS-18881	Flushing MAC address tables multiple times in a very short period of time can cause undefined BCM internal errors on VSP 8600 Series.	Wait at least 10 seconds between MAC flushes on VSP 8600 Series.
VOSS-22520	MACsec MKA sessions intermittently bounce on all ports when an IOC module is reset, even if MACsec MKA is disabled on the module being reset.	No workaround.

Issue number	Description	Workaround
VOSS-22593	When a packet bigger than MTU size is received on MACsec enabled ports, both the TooLong and the TooShort counters are incremented.	No workaround.
VOSS-22643	When an IOC module has all 6 software versions occupied and joins a chassis with a Primary CP that has 6 different software versions, the system displays an error message and does not boot.	Insert the IOC module as a Primary CP, remove at least one version from the module.
VOSS-22668	When a 1000Base-T GBIC module is inserted into a 8624XS IOC module, the port LED blinks without a cable plugged in.	No workaround. No functional impact.
VOSS-22924	Temporary traffic loss when bouncing IS-IS on BN pair with multicast traffic on channelized ports between VSP 8600 Series switches.	No workaround. Traffic recovers within four minutes.
VOSS-22995	After an IOC module slot reset, a COP-SW ERROR can appear for the local ARP of a VLAN with Fabric Connect multicast enabled. The ARP is programmed correctly, the error can be disregarded.	No workaround. No functional impact.
VOSS-22971	PIM traffic loss can occur in sVIST scenario after HA switchover in hot standby mode. Affects traffic from one peer for single home receivers connected to the other vIST peer. Ports from other slots are not affected.	You can bounce the connection of the affected port.
VOSS-23110	During a DVR controller reboot, some of the advertised hosts can disappear from other controllers in other DVR domains. The hosts are restored when the DVR controller is online.	No workaround.
VOSS-26505	The SPBM network does not support multiple multicast streams with the same source address and group address (S,G) learned on a VSP 8600 Series source BEB on multiple VLANs in the same VRF.	No workaround.

Filter Restrictions and Expected Behaviors

This section lists known restrictions and expected behaviors that can 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.

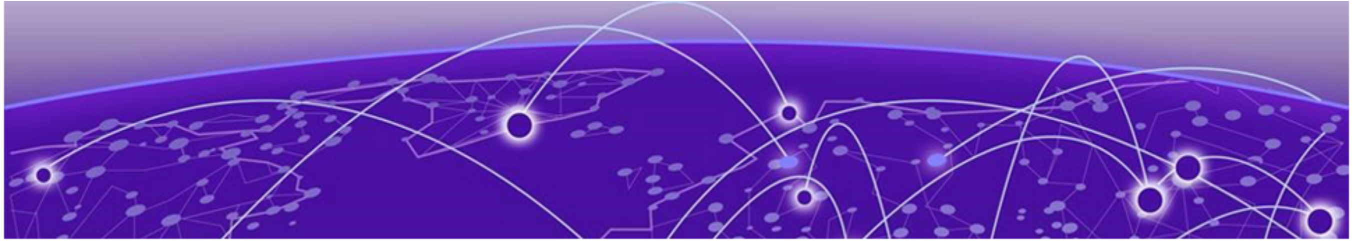
  For ACEs of VLAN-based ACLs, you can configure port qualifiers. Configuring VLAN qualifiers are not permitted.

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 *VOSS User Guide*.



Resolved Issues

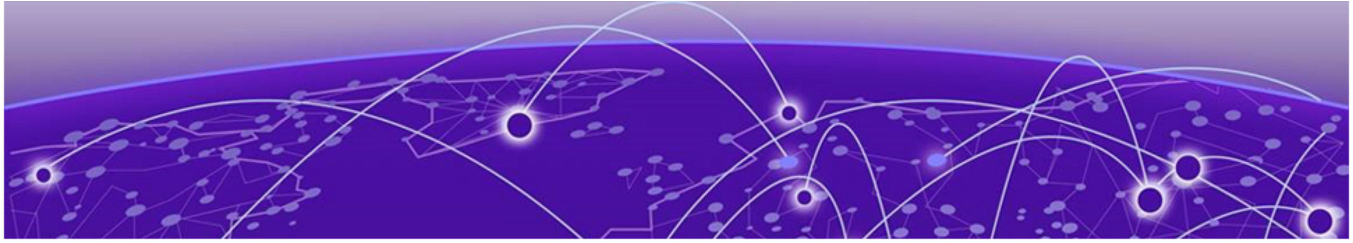
This section details the issues that are resolved in this release.

Fixes from previous releases

VSP 8600 Series Release 8.1 incorporates all fixes from prior releases, up to and including VSP 8600 Series Release 8.0.3.0.

Resolved issues in VSP 8600 Series 8.1

Issue number	Description
VOSS-21704	Core during software upgrade.
VOSS-22527	Logging wrong CardType detected constantly.
VOSS-22850	vIST went down breifly and recovered on own.
VOSS-22953	Port 1 - 4 on 8616QQ does not link up with 40GbiDiMMF is connected.
VOSS-23203	**`show cli username`** shows incorrect state after rebooting.
VOSS-24923	HCK WARNING missing heartbeats for process cbcp-main.x
VOSS-24929	SysUpTime counter roll over (after aproximately 497 days) causing high CPU utilization.



Related Information

The following section contains information related to the current release.

New MIBs

Table 13:

Object Name	Object OID
rcMACSecMKAProfileIncludeSCIEnable	1.3.6.1.4.1.2272.1.88.3.1.9
rcCliEnablePasswordSha2Mode	1.3.6.1.4.1.2272.1.19.45