ExtremeSwitching™

Release Notes for VSP 8600

Release 6.3
9035730 Rev AE
October 2020

Legal Notice

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

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

Trademarks

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

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

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

Open Source Declarations

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

Contents

Chapter 1: About this Document

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

Purpose

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

This document includes the following information:

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

Conventions

This section discusses the conventions used in this guide.

Text Conventions

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

Table 1: Notice Icons

Icon	Alerts you to...
! **Important:**	A situation that can cause serious inconvenience.
* **Note:**	Important features or instructions.

Table continues…

Icon	Alerts you to...
⊕ **Tip:**	Helpful tips and notices for using the product.
⚠ **Danger:**	Situations that will result in severe bodily injury; up to and including death.
⚠ **Warning:**	Risk of severe personal injury or critical loss of data.
⚠ **Caution:**	Risk of personal injury, system damage, or loss of data.

Table 2: Text Conventions

Convention	Description
Angle brackets (< >)	Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. If the command syntax is `cfm maintenance-domain maintenance-level <0-7>` , you can enter `cfm maintenance-domain maintenance-level 4`.
Bold text	Bold text indicates the GUI object name you must act upon. Examples: • Click **OK**. • On the **Tools** menu, choose **Options**.
Braces ({ })	Braces ({ }) indicate required elements in syntax descriptions. Do not type the braces when you enter the command. For example, if the command syntax is `ip address {A.B.C.D}`, you must enter the IP address in dotted, decimal notation.
Brackets ([ ])	Brackets ([ ]) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command. For example, if the command syntax is `show clock [detail]`, you can enter either `show clock` or `show clock detail`.
Ellipses (…)	An ellipsis (…) indicates that you repeat the last element of the command as needed. For example, if the command syntax is `ethernet/2/1 [ <parameter>`

Table continues…

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

Documentation and Training

Find Extreme Networks product information at the following locations:

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

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

Getting Help

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

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

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

Call GTAC For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

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

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

Subscribing to Service Notifications

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

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

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

4. Click **Submit**.

Providing Feedback to Us

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

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

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

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

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

Chapter 2: New in this release

New in this Release

The following sections detail what is new in VSP 8600 Series Release 6.3. For a full list of features, see Features by Release on page 39.

Transceivers

This release introduces support for the following transceiver modules and direct-attach cables.

40 Gb direct-attach cables:

- QSFP+ passive copper cable (PN: 10311), 0.5 meter
- QSFP+ active optical cable (PN: 10316), 20 meters

100 Gb direct-attach cables:

- QSFP28 active optical cable (PN: 10437), 20 meters

100 Gb transceiver modules:

- 100 Gb SWDM4 QSFP28 (PN: 10406)
- 100 Gb CWDM4-Lite 500m SMF QSFP28 (PN: 10450) *Requires FEC cl91

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

Extreme Networks optical transceivers and components	*Extreme Networks Pluggable Transceivers Installation Guide*
Compatibility for Extreme Networks SFP, SFP+, SFP28, QSFP+, and QSFP28 transceiver modules with the VSP Series switches	*Extreme Hardware/Software Compatibility and Recommendation Matrices*

Fabric Area Network (FAN)

Fabric Area Network (FAN) transit refers to the ability of a switch to forward traffic between SPB nodes participating in a FAN. The switch is neither a part of the FAN nor does it originate or sink FAN traffic. It only forwards the traffic between the FAN end-points.

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

Fabric Attach Server

This release introduces support for the Fabric Attach (FA) Server. When a switch is enabled as an FA Server, it receives IEEE 802.1AB Logical Link Discovery Protocol (LLDP) messages from FA Client and FA Proxy devices requesting the creation of Switched UNI service identifiers (I-SIDs). One FA Server can receive requests and consequently attach to multiple FA Client or Proxy devices.

Similarly, a single client or proxy device can connect to multiple switches in SMLT configuration acting as the FA Server. The I-SIDs thus created, are able to join a Shortest Path Bridging (SPB) network.

The FA Server automatically creates Switched UNI I-SIDs and endpoints for port and MLT interfaces on which the feature is enabled and mapping requests are received.

Both manually configured Switched UNI and automatically created FA I-SIDs and endpoints can co-exist on the same switch.

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

High Availability-CPU (HA-CPU) support in Simplified vIST

HA-CPU in Simplified vIST configurations enables synchronization of data for Layer 2 and Layer 3 applications between the master CPU and standby CPU, to provide hot standby capability.

For more information, see Administering VOSS.

Switched UNI

This release introduces a new type of Flex-UNI, called Switched UNI (S-UNI). The Switched UNI type helps you manually create an I-SID and map many VLAN IDs and port or MLT lists to that I-SID. The I-SIDs thus created are ELAN I-SIDs.

I-SID is IEEE next generation VLAN. SPB supports 16 million unique services where as the VLAN supports 4096. SPB I-SID is a true service ID and once it is provisioned at the edge, the network core automatically interconnects like I-SID endpoints to create a contiguous service.

Note:

You cannot enable EAPoL on Switched UNI ports because EAPoL does not support tagging and Switched UNI requires that the ports be tagged.

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

Transparent Port UNI

This release introduces support for Transparent Port User-Network-Interface (Transparent Port UNI or T-UNI). This feature enables you to map an entire port or an MLT to an I-SID. CMAC learning is done against the I-SID. T-UNI configures a transparent port where all traffic is MAC switched on an internal virtual port using the assigned I-SID. No VLAN is involved in this process. Devices switch tagged and untagged traffic in the assigned I-SID regardless of the VLAN ID. The T-UNI port or MLT can be either static or LACP and is not a member of any VLAN or Spanning Tree Group (STG). The T-UNI port or MLT is always in the forwarding state.

You can map multiple ports to a T-UNI I-SID. Multiple ports on the same switch and on other BEBs can use the common I-SID to switch traffic.

T-UNI is a point to point service and all traffic that ingress the UNI egress from the remote UNI end-point.

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

Filenames for this Release

Important:

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

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

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	VOSS8600.6.3.0.0.sha512	1714 bytes
MD5 Checksum files	VOSS8600.6.3.0.0.md5	658 bytes
MIB - supported object names	VOSS8600.6.3.0.0_mib_sup.txt	998,506 bytes
MIB - zip file of all MIBs	VOSS8600.6.3.0.0_mib.zip	1,087,451 bytes
MIB - objects in the OID compile order	VOSS8600.6.3.0.0_mib.txt	7,210,241 bytes
EDM Help files	VOSS86v630_HELP_EDM_gzip.zip	4,089,687 bytes
Logs reference	VOSS8600.6.3.0.0_edoc.tar	64,573,440 bytes
Software image	VOSS8600.6.3.0.0.tgz	149,763,245 bytes

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

Table 4: Open Source Software Files

Master copyright file	Open source base software
VOSS8600.6.3.0.0_oss-notice.html 2,526,400 bytes	VOSS8600.6.3.0.0_OpenSource.zip 95,862,435 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.

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, 6.1 or 6.2 to VSP 8600 Series 6.3.

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.

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.

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.

Chapter 4: 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
EC8602001-E6	VSP 8608	4.5.0.0	Y	Y	Y
EC8602002-E6	VSP 8608 with 3 SF modules and 4 AC PSUs	4.5.0.0	Y	Y	Y
EC8602003-E6	VSP 8608 DC with 3 SF modules and 4 DC PSUs	4.5.0.0	Y	Y	Y
EC8604001–E6	8600SF	4.5.0.0	Y	Y	Y
EC8604002-E6	8624XS	4.5.0.0	Y	Y	Y
EC8604003-E6	8624XT	4.5.0.0	Y	Y	Y
EC8604004-E6	8616QQ	4.5.0.0	Y	Y	Y
EC8604005-E6	8606CQ	4.5.0.1	Y	Y	Y

Chapter 5: Software Scaling

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

Layer 2

Table 5: 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
Switched UNI I-SIDs per switch (L2 only)	6000
Switched UNI endpoints per interface (same I-SID)	1
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

BGP+ peers	16
DHCP Relay forwarding entries (IPv4 or IPv6)	512 per VRF/1,024 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 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 7: 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 8: IP Multicast Maximums

<table>
<tr><td>IGMP interfaces</td><td>4,000</td></tr>
<tr><td>PIM interfaces (Active/Passive)</td><td>512/3,000</td></tr>
<tr><td>Multicast receivers/IGMP receiver entries (per switch)</td><td>6,000*</td></tr>
<tr><td colspan="2"><b>Note:</b>
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.</td></tr>
<tr><td>Multicast senders/IGMP sender entries (per switch)</td><td>6,000</td></tr>
<tr><td>PIM-SSM static channels</td><td>4,000</td></tr>
<tr><td>Total multicast routes (S,G,V) (per switch)</td><td>6,000</td></tr>
</table>

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 9: 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 10: 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.	
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
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 11: OAM and Diagnostics Maximums

EDM sessions	5
FTP sessions	4
Mirrored destination ports	4

Table continues…

Mirroring ports	191
Rlogin sessions	8
sFlow sampling rate	5000 samples per second per IOC module
SSH sessions	8
Telnet sessions	8

Chapter 6: 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.
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.

Table continues…

Offer Level	Period	Support
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) • Greater than 24 VRFs • Greater than 16 BGP Peers Layer 3 Virtualization with MACsec: • Layer 3 Virtual Services Networks (VSNs) • Greater than 24 VRFs • Greater than 16 BGP Peers • MACsec

For more information about licenses, see Administering VOSS.

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 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.

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	**`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.
VOSS-6104	**`sys action`** reset counters command does not reset any ISIS system stats.	Use `clear isis` 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-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.
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 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	No workaround, but there is no operational impact.

Table continues…

Issue number	Description	Workaround
	mismatch if the switch is running release 6.1.x or higher and it has an IOC running release 4.5.x.	
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: 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: `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 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). Filter statistics increment normally if the packet is not marked for drop or if the packet does not	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.

Table continues…

Issue number	Description	Workaround
	contain a mirroring action (even if the packet is marked for drop).	
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.
VOSS-10091	After deleting an IPVPN, you may 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 may 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.

Table continues…

Issue number	Description	Workaround
VOSS-10802	The **show app-telemetry status** command incorrectly displays the Collector status as `not reachable`. 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.	Avoid configurations where the sFlow collector is reachable through both the MGMT and GRT.
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**.
VOSS-10876	Application Telemetry reachability information is not available from EDM.	Check the logs or use the CLI **show app-telemetry status** command.
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 appears 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 appears and traffic is hashed to	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.

Table continues…

Issue number	Description	Workaround
	B, there will be minimal traffic outage until B creates the distribution tree on the SPBM core.	
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 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-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-12573	If a Layer 3 S-UNI port has untagged BPDU enabled and at the same time has a platform VLAN configured on a different I-SID, ARP Learning does not work on that platform VLAN.	Disable untagged BPDU on the port for ARP Learning to work.
VOSS-12953 VOSS-13898	The system sometimes displays the following message: `HW INFO Detected Unknown Card Type module in slot`	No workaround, but there is no operational or functional impact.
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.	Power on one card at a time.
VOSS-13789	A link between a channelized 100 Gbps port on the VSP 8600 Series and a 25 Gbps port on the VSP 7400-48Y is not established, when you use a 100 Gbps to 25 Gbps direct-attach copper breakout cable.	To restore the link, you must disable Auto-Negotiation and FEC on the 25 Gbps port on the VSP 7400-48Y.

Table continues…

Issue number	Description	Workaround
VOSS-13856	The system sometimes sends traffic packets with the time-to-live (TTL) set to zero.	No workaround, but there is no operational impact or impact to traffic.
VOSS-13921	When you remove a card from the VSP 8600 chassis, you may see the following warning message: `GlobalRouter LMF WARNING lmfUpdateEgressIpmcSession () Null receiver port for subintf null egress vlan 334`.	No workaround, but there is no operational impact or impact to traffic.

VOSS-13924	You may sometimes see the following log messages warning you about SMLT send-queue utilization. These messages appear even if the problem doesn't exist, and can be repetitive.
	`1 2019-05-30T13:46:03.941-04:00 wolfboro-1 CP1 - 0x00064724 - 00000000 GlobalRouter MLT WARNING SMLT buffer usage over 200M. Low memory warning condition`
	`1 2019-05-30T13:46:03.941-04:00 wolfboro-1 CP1 - 0x00064726 - 00000000 GlobalRouter MLT INFO DBG info for SMLT high mem: istSmltSendBufFullFail 7179242 istSocketWaitingForRestOfMsg 878243 istRxLearnMacCnt 24456 istTxLearnMacCnt 72888`
	`1 2019-05-30T13:46:46.999-04:00 wolfboro-1 CP1 - 0x00064725 - 00000000 GlobalRouter MLT INFO SMLT buffer usage under 100M, clearing low memory condition`
		No workaround, but there is no functionality impact.

VOSS-13954	In a scaled FA environment (with nearly 2000 ELAN I-SIDs on a single homed UNI port), if you disable and enable FA on the chassis in quick succession, there is intermittent loss of traffic on the FA endpoints. This issue is seen only if all endpoints are Layer 2 VSN endpoints and scaled close to the limit of 2000 endpoints on a singled homed UNI port. This issue is not seen if a platform VLAN is associated with an I-SID. This issue is also not seen if you disable FA, wait for the endpoints to be cleaned up, and then enable FA.	In a scaled FA environment, when you bring down a port, ensure that all FA endpoints are cleared using the command **`show i-sid elan`**, before you enable the port back up again.

Table continues…

Issue number	Description	Workaround
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-14085	When you disable and then enable vIST, the following event synchronization failure log messages are displayed on the hot standby CPU: `Application Sync failed for entity: 0x504c5342 representing Module PLSB ,event:5/3 maxNumEvents:6Event sync failed to add MGID <Mgid number> to the mgid map using lanemask 0x1000 as index on standby CP` This failure is observed when you disable and enable vIST and may be observed in other scenarios also. It occurs because the MGID is already updated on the standby CPU when synchronization from the master CPU is received.	No workaround, but there is no functional impact.
VOSS-14094	When you power on/off a card using the CLI, traffic does not recover on FA-enabled MLTs with member ports on a single I/O slot, because the MLT members are not programmed in the data-path. This issue is seen only when you power on/off the card and is not seen when you reset the card, or physically insert into or remove from the slot. This issue is also not seen on the following: • SMLT ports • An MLT that has at least one port on a different slot. • A single non-MLT port. • A port that is not FA-enabled.	Use the following procedure: 1. Disable FA on the MLT first. 2. Power on/off the card on the chassis. Wait for it to finish powering on/off completely. 3. Re-enable FA on the MLT.

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 for VOSS.

Chapter 8: Resolved Issues

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

Fixes from previous releases

VSP 8600 Series 6.3 incorporates all fixes from prior releases.

Resolved issues in VSP 8600 Series 6.3

Issue number	Description
VOSS-11071	If you toggle an SF or I/O module off and on (sys power) and perform a CP switchover in parallel (sys action cpu-switch-over), the show **`sys-info command`** displays the Power State as `Off` even though Oper status and Admin status are `UP`. 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-11521	EDM does not display the Card HW Revision number correctly.
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 an CPU switch-over. Problem corrects itself after the next periodic mac sync from vist peer.
VOSS-12053	VLAN based traffic filtering does not work either on a T-UNI port or on a C-VLAN port that is converted to a T-UNI port.
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.
VOSS-10473	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.
VOSS-10544	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.` This issue has no impact on the switch operation.
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.
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`.

Table continues…

Issue number	Description
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.
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.
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.
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.
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.
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.
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.
VOSS-13257	In the warm-standby mode, when the master CPU card is removed from the slot, the ports on the card do not go down immediately during a reset.

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 introduced
Access Control List (ACL)-based filtering: • Egress ACLs • Ingress ACLs • Layer 2 to Layer 4 filtering • Port-based • VLAN-based For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	4.5
Address Resolution Protocol (ARP): • Proxy ARP • Static ARP For more information, see Configuring IPv4 Routing for VOSS.	4.5
Advanced Feature Bandwidth Reservation	Not supported
Alternative routes for IPv4 For more information, see Configuring IPv4 Routing for VOSS.	4.5
Alternative routes for IPv6 For more information, see Configuring IPv6 Routing for VOSS.	6.2
Application Telemetry For more information, see Monitoring Performance for VOSS.	6.2

Table continues…

Feature	Release introduced
Automatic QoS For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	4.5
Border Gateway Protocol for IPv4 (BGPv4) For more information, see Configuring BGP Services for VOSS.	4.5
BGP+ (BGPv4 for IPv6) For more information, see Configuring BGP Services for VOSS.	6.2
BGPv6	Not supported
Bridge Protocol Data Unit (BPDU) Guard For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS.	6.2
Certificate order priority	Not supported
CFM configuration on C-VLANs	Not supported
Channelization of 40 Gbps ports For more information, see the hardware documentation and Administering VOSS.	6.1
Channelization of 100 Gbps ports For more information, see the hardware documentation and Administering VOSS.	6.2
Command Line Interface (CLI) For more information, see Configuring User Interfaces and Operating Systems for VOSS.	4.5
Differentiated Services (DiffServ) including Per-Hop Behavior For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	4.5
Digital Certificate/PKI For more information, see Configuring Security for VOSS.	6.1
Directed Broadcast	Not supported
Distributed Virtual Routing (DvR) controller	Not supported
Distributed Virtual Routing (DvR) leaf	Not supported
DNS client (IPv6) For more information, see Administering VOSS.	6.2
Domain Name Service (DNS) client (IPv4) For more information, see Administering VOSS.	4.5
Dot1Q MIB • dot1VlanCurrentTable	6.1

Table continues…

Feature	Release introduced
• dot1qVlanStaticTable • dot1qPortVlanTable • dot1dBasePortEntry • dot1qVlanNumDelete	
Dynamic Host Configuration Protocol (DHCP) Relay, DHCP Option 82 For more information, see Configuring IPv4 Routing for VOSS.	4.5
DHCP Snooping (IPv4)	Not supported
DHCP Snooping (IPv6)	Not supported
DHCPv6 Guard	Not supported
Dynamic ARP Inspection (DAI)	Not supported
Dynamic Nickname Assignment	Not supported
Egress port mirror For more information, see Troubleshooting VOSS.	4.5
Egress port shaper For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	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.	Not supported
Energy Saver	Not supported
EDM representation of physical LED status For more information, see Installing the Virtual Services Platform 8600.	4.5
Entity MIB enhancements and integration for the following: • Physical Table • Alias Mapping Table • Physical Contains Table • Last Change Time Table For more information, see Administering VOSS.	6.1
Equal Cost Multiple Path (ECMP) for IPv4 For more information, see Configuring IPv4 Routing for VOSS.	4.5
ECMP for IPv6 For more information, see the following documents: • Configuring IPv4 Routing for VOSS • Configuring BGP Services for VOSS	6.2

Table continues…

Feature	Release introduced
• Configuring IPv6 Routing for VOSS	
ECMP support for Fabric Extend	Not supported
ECMP support for VXLAN Gateway and Fabric Extend	Not supported
Equal Cost Trees (ECT) For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	4.5
E-Tree and Private VLANs	Not supported
Extensible Authentication Protocol (EAP) and EAP over LAN (EAPoL)	Not supported
EAPoL MHMA-MV	Not supported
EAPoL enhancements: Enhanced MHMV, Fail Open VLAN, Guest VLAN	Not supported
External BGP (EBGP) For more information, see Configuring BGP Services for VOSS.	4.5
Extreme Management Center backup configuration ZIP file For more information, see Extreme Management Center documentation.	6.1
Fabric Attach Server For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	6.3
Fabric Attach Zero Touch Client Attachment For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	6.3
Fabric BCB mode For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	4.5
Fabric BEB mode For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	6.1
Fabric Connect services with switch cluster For more information, see the Fabric Connect documents: • Configuring Fabric Basics and Layer 2 Services for VOSS • Configuring Fabric Layer 3 Services for VOSS • Configuring Fabric Multicast Services for VOSS	6.1
Fabric Extend	Not supported
Fabric RSPAN (Mirror to I-SID)	Not supported
File Transfer Protocol (FTP) server and client (IPv4) For more information, see Administering VOSS.	4.5
File Transfer Protocol (FTP) server and client (IPv6)	6.2

Table continues…

Feature	Release introduced
For more information, see Administering VOSS.	
First Hop Security (FHS)	Not supported
FHS - DHCPv6 Guard	Not supported
FHS - DHCP Snooping (IPv4)	Not supported
FHS - DHCP Snooping (IPv6)	Not supported
FHS - IP Source Guard (IPv4 and IPv6)	Not supported
FHS - Neighbor Discovery Inspection (IPv6)	Not supported
FHS - IPv6 Router Advertisement (RA) Guard	Not supported
Flight Recorder for system health monitoring For more information, see Troubleshooting VOSS.	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 Configuring IPv4 Routing for VOSS.	4.5
High Availability CPU (HA-CPU) for a standalone switch For more information, see Administering VOSS.	4.5
High Availability CPU (HA-CPU) for Layer 2 with Simplified vIST For more information, see Administering VOSS.	6.3
High Availability CPU (HA-CPU) for Layer 3 with Simplified vIST For more information, see Administering VOSS.	6.3
Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) (IPv4)	4.5
Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) (IPv6)	6.2
IEEE 802.1AG Connectivity Fault Management (CFM): • Layer 2 Ping • TraceRoute • TraceTree For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	4.5
IEEE 802.3X Pause frame transmit	Not supported
Industry Standard Discovery Protocol (ISDP) (CDP compatible)	Not supported
Ingress dual rate port policers For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	4.5

Table continues…

Feature	Release introduced
Internal BPG (IBGP) For more information, see Configuring BGP Services for VOSS.	4.5
Internet Control Message Protocol (ICMP) For more information, see Configuring IPv4 Routing for VOSS.	4.5
InVSN Filter	Not supported
ICMP broadcast and multicast enable or disable For more information, see Configuring IPv4 Routing for VOSS and Configuring IPv6 Routing for VOSS.	4.5
Internet Group Management Protocol (IGMP), including virtualization For more information, see Configuring IP Multicast Routing Protocols for VOSS.	4.5
Internet Key Exchange (IKE) v2	Not supported
Inter-VSN routing (IPv4) For more information, see Configuring Fabric Layer 3 Services for VOSS.	6.1
Inter-VSN routing (IPv6)	Not supported
IP Multicast over Fabric Connect For more information, see Configuring Fabric Multicast Services for VOSS.	6.2
IP route policies For more information, see Configuring IPv4 Routing for VOSS.	4.5
IP Shortcut routing including ECMP For more information, see Configuring Fabric Layer 3 Services for VOSS.	6.1
IP Source Guard (IPv4 and IPv6)	Not supported
IP Source Routing enable or disable For more information, see Configuring IPv4 Routing for VOSS and Configuring IPv6 Routing for VOSS.	4.5
IPsec transport mode	Not supported
IPsec for the Out-of-band management port (IPv4)	Not supported
IPsec for the Out-of-band management port (IPv6)	Not supported
IPv6 (OSPFv3, VRRP, RSMLT, DHCP Relay, IPv4 in IPv6 tunnels) For more information, see Configuring IPv6 Routing for VOSS.	6.2
IPv6 ACL filters For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	6.2 (on Ingress only)
IPv6 egress filters	Not supported
IPv6 mode flag (**`boot config flags ipv6-mode`**)	Not supported

Table continues…

Feature	Release introduced
IPv6 Shortcut routing	Not supported
IPv6 Virtualization for the following features and functions: • 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	Not supported
IPv4 IS-IS accept policies For more information, see Configuring Fabric Layer 3 Services for VOSS.	6.1
IPv6 IS-IS accept policies	Not supported
IS-IS authentication with SHA-256 For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	6.1
Key Health Indicator (KHI) For more information, see Monitoring Performance for VOSS.	4.5
Layer 2 Video Surveillance install script	Not supported
Layer 3 Video Surveillance install script (formerly known as the run vms endura script)	Not supported
Layer 2 Virtual Service Network (VSN) For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	4.5
Layer 3 switch cluster (Routed SMLT) with Simplified vIST For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.	4.5
Layer 3 switch cluster (Routed SMLT) with Virtual Inter-Switch Trunk (vIST) For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.	6.1
Layer 3 VSN For more information, see Configuring Fabric Layer 3 Services for VOSS.	6.1
linerate-directed-broadcast boot flag (**`boot config flags linerate-directed-broadcast`**)	Not supported
Link Layer Discovery Protocol (LLDP) For more information, see Administering VOSS.	6.1
Link Layer Discovery Protocol- Media Endpoint Discovery (LLDP-MED)	Not supported
Link-state tracking (LST)	Not supported

Table continues…

Feature	Release introduced
Linux kernel version 4.9	Not supported
Logging to a file and syslog (IPv4) For more information, see Monitoring Performance for VOSS.	4.5
Logging to a file and syslog (IPv6) For more information, see Monitoring Performance for VOSS.	6.2
Logon banner For more information, see Administering VOSS. **Note:** Configurable using CLI only.	4.5
MAC security (MAC-layer filtering, limit learning)	Not supported
MACsec 2AN mode	Not supported
MACsec 4AN mode For more information, see Configuring Security for VOSS.	4.5
Mirroring (port and flow-based) For more information, see Troubleshooting VOSS.	4.5
MSTP-Fabric Connect Multi Homing	Not supported
Multicast Listener Discovery (MLD)	Not supported
Multicast route (mroute) statistics for IPv4 and IPv6	Not supported
MultiLink Trunking (MLT) / Link Aggregation Group (LAG) For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.	4.5
Multiple CLI users per role	Not supported
Multiple IS-IS parallel adjacencies	Not supported
Neighbor Discovery Inspection (IPv6)	Not supported
Network Load Balancing (NLB) - multicast operation	Not supported
Network Load Balancing (NLB) - unicast operation For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS.	4.5
Network Time Protocol version 3 (NTPv3) For more information, see Administering VOSS.	4.5
nni-mstp boot flag (`boot config flags nni-mstp`) **Important:** This flag has special upgrade considerations the first time you upgrade to a release that supports it.	Not supported
Non EAPoL MAC RADIUS authentication	Not supported

Table continues…

Feature	Release introduced
NTPv3	4.5
NTPv3 with SHA authentication	4.5
NTPv4 for IPv4	Not supported
NTPv4 for IPv6	Not supported
Open Shortest Path First (OSPF) For more information, see Configuring OSPF and RIP for VOSS.	4.5
OVSDB protocol support for VXLAN Gateway	Not supported
P-Bridge MIB Adds support for: • dot1dExtBase Group • dot1dDeviceCapabilities • dot1dTrafficClassesEnabled • dot1dGmrpStatus • dot1dPortCapabilitiesTable	6.1
Protocol Independent Multicast-Sparse Mode (PIM-SM), PIM-Source Specific Mode (PIM-SSM) for IPv4 For more information, see Configuring IP Multicast Routing Protocols for VOSS.	4.5
PIM and PIM-SSM over IPv6	Not supported
Power Management	Not supported
Power over Ethernet (PoE)	Not supported
PoE/PoE+ allocation using LLDP	Not supported
QoS Access Control Entries (ACE) For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	6.2
QoS ingress port rate limiter	Not supported
QoS Priority Assignment	Not supported
RADIUS (IPv6) For more information, see Configuring Security for VOSS.	6.2
RADIUS attributes: • Acct-Terminate-Cause • Event-Timestamp • Service Type	Not supported
RADIUS, community-based users (IPv4) For more information, see Configuring Security for VOSS.	4.5

Table continues…

Feature	Release introduced
RADIUS secure communication using IPSec for IPv4	Not supported
RADIUS secure communication using IPSec for IPv6	Not supported
Read-Only user for EDM	Not supported
Remote Login (Rlogin) server/client (IPv4) For more information, see Administering VOSS.	4.5
Rlogin server (IPv6) For more information, see Administering VOSS.	6.2
Rlogin client (IPv6)	Not supported
Remote Monitoring 1 (RMON1) for Layer 1 and Layer 2 For more information, see Monitoring Performance for VOSS.	4.5
Remote Monitoring 2 (RMON2) for network and application layer protocols	Not supported
Remote Shell (RSH) server/client For more information, see Administering VOSS.	4.5
RFC 5176 – Dynamic Authorization Extensions to RADIUS	Not supported
RFC 5997 – RADIUS Reachability Server Status	Not supported
Route Information Protocol (RIP) For more information, see Configuring OSPF and RIP for VOSS.	4.5
RIPng For more information, see Configuring IPv6 Routing for VOSS.	6.2
run spbm installation script	Not supported
Secure Copy (SCP) **Note:** The switch does not support the WinSCP client. For more information, see Administering VOSS.	4.5
Secure hash algorithm 1 (SHA-1) and SHA-2 For more information, see Configuring OSPF and RIP for VOSS.	4.5
Secure Shell (SSH) server (IPv4) For more information, see Administering VOSS.	4.5
Secure Shell (SSH) client (IPv4) For more information, see Administering VOSS.	4.5
Secure Sockets Layer (SSL) certificate management For more information, see Administering VOSS.	4.5
SSH server (IPv6)	6.2
SSH client (IPv6)	Not supported

Table continues…

Feature	Release introduced
Security ACEs For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS.	4.5
Segmented Management Instance	Not supported
sFlow For more information, see Monitoring Performance for VOSS.	6.2
sFlow collector reachability on user-created VRFs For more information, see Monitoring Performance for VOSS.	6.2
Simple Loop Prevention Protocol (SLPP) For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS.	4.5
Simple Mail Transfer Protocol (SMTP) for log notification For more information, see Monitoring Performance for VOSS.	6.1
Simple Network Management Protocol (SNMP) v1/2/3 (IPv4) For more information, see Configuring Security for VOSS.	4.5
SLA Mon For more information, see Configuring the SLA Mon Agent for VOSS.	4.5
SLPP Guard For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.	6.2
SNMP (IPv6) For more information, see Configuring Security for VOSS.	6.2
SoNMP For more information, see Administering VOSS.	4.5
Spanning Tree Protocol (STP): • Multiple STP (MSTP) • Rapid STP (RSTP) For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS.	4.5
spbm-config-mode (`boot config flags spbm-config-mode`) For more information, see Configuring IP Multicast Routing Protocols for VOSS.	4.5
SPB-PIM Gateway controller node	Not supported
SPB-PIM Gateway interface	Not supported
SSH (IPv6)	6.2

Table continues…

Feature	Release introduced
For more information, see Administering VOSS.	
SSH client disable For more information, see Administering VOSS.	4.5
SSH key size For more information, see Administering VOSS.	6.1
SSH rekey For more information, see Administering VOSS.	6.1
Static routing For more information, see Configuring IPv4 Routing for VOSS.	4.5
Suspend duplicate system ID detection For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	6.1
Switch cluster (multi-chassis LAG) -Virtual Inter-Switch Trunk (vIST) For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.	6.1
Switched UNI (S-UNI) For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	6.3
TACACS+ For more information, see Configuring Security for VOSS.	4.5
TACACS+ secure communication using IPSec for IPv4	Not supported
Telnet server and client (IPv4) For more information, see Administering VOSS.	4.5
Telnet server and client (IPv6) For more information, see Administering VOSS.	6.2
TLS server for secure HTTPS For more information, see Configuring User Interfaces and Operating Systems for VOSS.	6.1
TLS client for secure syslog	Not supported
Transparent Port UNI (T-UNI) For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.	6.3
Trivial File Transfer Protocol (TFTP) server and client (IPv4) For more information, see Administering VOSS.	4.5
TFTP client (IPv6)	Not supported
TFTP server (IPv6)	6.2

Table continues…

Feature	Release introduced
For more information, see Administering VOSS.	
Unicast Reverse Path Forwarding (URPF) checking (IPv4 and IPv6) **Note:** Supported on IPv4 only. For more information, see Configuring Security for VOSS.	4.5
Virtual Inter-Switch Trunk (vIST) For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.	6.1
Virtual Link Aggregation Control Protocol (VLACP) For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.	4.5
Virtual Router Redundancy Protocol (VRRP) For more information, see Configuring IPv4 Routing for VOSS.	4.5
Virtualization with IPv4 Virtual Routing and Forwarding (VRF) • ARP • DHCP Relay • Inter-VRF Routing (static, dynamic, and policy) • Local routing • OSPFv2 • RIPv1 and v2 • Route policies • Static routing • VRRP For more information, see Configuring IPv4 Routing for VOSS.	4.5
Increased VRF and Layer 3 scaling (The VSP 8600 automatically supports the maximum number of VRFs without additional VLAN reservation.)	Not supported
VRRPv3 for IPv4 and IPv6 For more information, see Configuring IPv4 Routing for VOSS and Configuring IPv6 Routing for VOSS.	6.1
VXLAN Gateway	Not supported
Zero Touch Fabric configuration	Not supported

MIB Changes

New MIBs

Object Name	Object OID
avayaFabricAttachMib	1.3.6.1.4.1.45.5.46
avFabricAttachObjects	1.3.6.1.4.1.45.5.46.1
avFabricAttachService	1.3.6.1.4.1.45.5.46.1.1
avFabricAttachElementType	1.3.6.1.4.1.45.5.46.1.2
avFabricAttachIsidVlanAsgnsTable	1.3.6.1.4.1.45.5.46.1.5
avFabricAttachIsidVlanAsgnsEntry	1.3.6.1.4.1.45.5.46.1.5.1
avFabricAttachIsidVlanAsgnsIfIndex	1.3.6.1.4.1.45.5.46.1.5.1.1
avFabricAttachIsidVlanAsgnsIsid	1.3.6.1.4.1.45.5.46.1.5.1.2
avFabricAttachIsidVlanAsgnsVlan	1.3.6.1.4.1.45.5.46.1.5.1.3
avFabricAttachIsidVlanAsgnsState	1.3.6.1.4.1.45.5.46.1.5.1.4
avFabricAttachIsidVlanAsgnsOrigin	1.3.6.1.4.1.45.5.46.1.5.1.6
avFabricAttachPortTable	1.3.6.1.4.1.45.5.46.1.6
avFabricAttachPortEntry	1.3.6.1.4.1.45.5.46.1.6.1
avFabricAttachPortIfIndex	1.3.6.1.4.1.45.5.46.1.6.1.1
avFabricAttachPortState	1.3.6.1.4.1.45.5.46.1.6.1.2
avFabricAttachPortRowStatus	1.3.6.1.4.1.45.5.46.1.6.1.3
avFabricAttachPortMsgAuthStatus	1.3.6.1.4.1.45.5.46.1.6.1.4
avFabricAttachPortMsgAuthKey	1.3.6.1.4.1.45.5.46.1.6.1.5
avFabricAttachPortMgmtIsid	1.3.6.1.4.1.45.5.46.1.6.1.6
avFabricAttachPortMgmtCvid	1.3.6.1.4.1.45.5.46.1.6.1.7
avFabricAttachDiscElemsTable	1.3.6.1.4.1.45.5.46.1.11
avFabricAttachDiscElemsEntry	1.3.6.1.4.1.45.5.46.1.11.1
avFabricAttachDiscElemsIfIndex	1.3.6.1.4.1.45.5.46.1.11.1.1
avFabricAttachDiscElemsElementType	1.3.6.1.4.1.45.5.46.1.11.1.2
avFabricAttachDiscElemsElementVlan	1.3.6.1.4.1.45.5.46.1.11.1.3
avFabricAttachDiscElemsElementId	1.3.6.1.4.1.45.5.46.1.11.1.4
avFabricAttachDiscElemsElementState	1.3.6.1.4.1.45.5.46.1.11.1.5
avFabricAttachDiscElemsElementAuth	1.3.6.1.4.1.45.5.46.1.11.1.6
avFabricAttachDiscElemsElementOperAuthStatus	1.3.6.1.4.1.45.5.46.1.11.1.8

Table continues…

Object Name	Object OID
avFabricAttachDiscElemsElementAsgnsOperAuthStatus	1.3.6.1.4.1.45.5.46.1.11.1.9
avFabricAttachDiscElemsAsgnsAuth	1.3.6.1.4.1.45.5.46.1.11.1.10
avFabricAttachProvisionMode	1.3.6.1.4.1.45.5.46.1.13
avFabricAttachAsgnTimeout	1.3.6.1.4.1.45.5.46.1.22
avFabricAttachStatsTable	1.3.6.1.4.1.45.5.46.1.23
avFabricAttachStatsEntry	1.3.6.1.4.1.45.5.46.1.23.1
avFabricAttachStatsPortIndex	1.3.6.1.4.1.45.5.46.1.23.1.1
avFabricAttachStatsDiscElemReceived	1.3.6.1.4.1.45.5.46.1.23.1.2
avFabricAttachStatsAsgnReceived	1.3.6.1.4.1.45.5.46.1.23.1.3
avFabricAttachStatsAsgnAccepted	1.3.6.1.4.1.45.5.46.1.23.1.4
avFabricAttachStatsAsgnRejected	1.3.6.1.4.1.45.5.46.1.23.1.5
avFabricAttachStatsAsgnExpired	1.3.6.1.4.1.45.5.46.1.23.1.6
avFabricAttachStatsDiscAuthFailed	1.3.6.1.4.1.45.5.46.1.23.1.7
avFabricAttachStatsDiscElemExpired	1.3.6.1.4.1.45.5.46.1.23.1.8
avFabricAttachStatsDiscElemDeleted	1.3.6.1.4.1.45.5.46.1.23.1.9
avFabricAttachStatsAsgnDeleted	1.3.6.1.4.1.45.5.46.1.23.1.10
avFabricAttachStatsAsgnAuthFailed	1.3.6.1.4.1.45.5.46.1.23.1.11
avFabricAttachGlobalStats	1.3.6.1.4.1.45.5.46.1.24
avFabricAttachGlobalStatsDiscElemReceived	1.3.6.1.4.1.45.5.46.1.24.1
avFabricAttachGlobalStatsAsgnReceived	1.3.6.1.4.1.45.5.46.1.24.2
avFabricAttachGlobalStatsAsgnAccepted	1.3.6.1.4.1.45.5.46.1.24.3
avFabricAttachGlobalStatsAsgnRejected	1.3.6.1.4.1.45.5.46.1.24.4
avFabricAttachGlobalStatsAsgnExpired	1.3.6.1.4.1.45.5.46.1.24.5
avFabricAttachGlobalStatsDiscAuthFailed	1.3.6.1.4.1.45.5.46.1.24.6
avFabricAttachGlobalStatsDiscElemExpired	1.3.6.1.4.1.45.5.46.1.24.7
avFabricAttachGlobalStatsDiscElemDeleted	1.3.6.1.4.1.45.5.46.1.24.8
avFabricAttachGlobalStatsAsgnDeleted	1.3.6.1.4.1.45.5.46.1.24.9
avFabricAttachGlobalStatsAsgnAuthFailed	1.3.6.1.4.1.45.5.46.1.24.10
avFabricAttachDiscTimeout	1.3.6.1.4.1.45.5.46.1.26
avFabricAttachZeroTouchClientTable	1.3.6.1.4.1.45.5.46.1.27
avFabricAttachZeroTouchClientEntry	1.3.6.1.4.1.45.5.46.1.27.1
avFabricAttachZeroTouchClientType	1.3.6.1.4.1.45.5.46.1.27.1.1
avFabricAttachZeroTouchClientDescr	1.3.6.1.4.1.45.5.46.1.27.1.2
avFabricAttachZeroTouchClientRowStatus	1.3.6.1.4.1.45.5.46.1.27.1.4

Table continues…

Object Name	Object OID
avFabricAttachZeroTouchClientName	1.3.6.1.4.1.45.5.46.1.27.1.5
avFabricAttachZeroTouchClientOrigin	1.3.6.1.4.1.45.5.46.1.27.1.6
avFabricAttachStats	1.3.6.1.4.1.45.5.46.1.28
avFabricAttachStatsClearErrorCounters	1.3.6.1.4.1.45.5.46.1.28.1
avFabricAttachStatsClearGlobalErrorCounters	1.3.6.1.4.1.45.5.46.1.28.2
avFabricAttachZeroTouchClientAttachTable	1.3.6.1.4.1.45.5.46.1.29
avFabricAttachZeroTouchClientAttachEntry	1.3.6.1.4.1.45.5.46.1.29.1
avFabricAttachZeroTouchClientAttachType	1.3.6.1.4.1.45.5.46.1.29.1.1
avFabricAttachZeroTouchClientAttachVlan	1.3.6.1.4.1.45.5.46.1.29.1.2
avFabricAttachZeroTouchClientAttachIsid	1.3.6.1.4.1.45.5.46.1.29.1.4
avFabricAttachZeroTouchClientAttachRowStatus	1.3.6.1.4.1.45.5.46.1.29.1.5
rcIsidElanTransparentTable	1.3.6.1.4.1.2272.1.87.3
rcIsidElanTransparentEntry	1.3.6.1.4.1.2272.1.87.3.1
rcIsidElanTransparentId	1.3.6.1.4.1.2272.1.87.3.1.1
rcIsidElanTransparentPortMembers	1.3.6.1.4.1.2272.1.87.3.1.2
rcIsidElanTransparentMltIds	1.3.6.1.4.1.2272.1.87.3.1.3
rcPortFlexUniEnable	1.3.6.1.4.1.2272.1.4.10.1.1.116
rcMltFlexUniEnable	1.3.6.1.4.1.2272.1.17.10.1.49
rcIsidElanEndPointTable	1.3.6.1.4.1.2272.1.87.4
rcIsidInterfaceTable	1.3.6.1.4.1.2272.1.87.5
rcIsidInterfaceEntry	1.3.6.1.4.1.2272.1.87.5.1
rcIsidInterfaceIfIndex	1.3.6.1.4.1.2272.1.87.5.1.1
rcIsidInterfaceIsid	1.3.6.1.4.1.2272.1.87.5.1.2
rcIsidInterfaceVlan	1.3.6.1.4.1.2272.1.87.5.1.3
rcIsidInterfaceCvid	1.3.6.1.4.1.2272.1.87.5.1.4
rcIsidInterfaceType	1.3.6.1.4.1.2272.1.87.5.1.5
rcIsidInterfaceOrigin	1.3.6.1.4.1.2272.1.87.5.1.6
rcIsidInterfaceBpdu	1.3.6.1.4.1.2272.1.87.5.1.7
rcBridgeIsidFdbCvid	1.3.6.1.4.1.2272.1.14.23.1.9
rcIpNetToMediaDestCvid	1.3.6.1.4.1.2272.1.8.30.1.10
rcBridgeTpFdbCvid	1.3.6.1.4.1.2272.1.14.20.1.9
rcIpv6NetToPhysicalCvid	1.3.6.1.4.1.2272.1.62.1.1.7.1.11
rcIsidElanEndPointEntry	1.3.6.1.4.1.2272.1.87.4.1
rcIsidElanEndPointIsid	1.3.6.1.4.1.2272.1.87.4.1.1
rcIsidElanEndPointCvid	1.3.6.1.4.1.2272.1.87.4.1.2

Table continues…

Object Name	Object OID
rcIsidElanEndPointIfIndex	1.3.6.1.4.1.2272.1.87.4.1.3
rcIsidElanEndPointRowStatus	1.3.6.1.4.1.2272.1.87.4.1.4
rcIsidElanEndPointBpdu	1.3.6.1.4.1.2272.1.87.4.1.5
rcIsidElanEndPointOrigin	1.3.6.1.4.1.2272.1.87.4.1.6
rcVxlanVnidElanEndPointTable	1.3.6.1.4.1.2272.1.218.7
rcVxlanVnidElanEndPointEntry	1.3.6.1.4.1.2272.1.218.7.1
rcVxlanVnidElanEndPointVnid	1.3.6.1.4.1.2272.1.218.7.1.1
rcVxlanVnidElanEndPointCvid	1.3.6.1.4.1.2272.1.218.7.1.2
rcVxlanVnidElanEndPointIfIndex	1.3.6.1.4.1.2272.1.218.7.1.3
rcVxlanVnidElanEndPointIsid	1.3.6.1.4.1.2272.1.218.7.1.4
rcVxlanVnidElanEndPointRowStatus	1.3.6.1.4.1.2272.1.218.7.1.5
rcBridgeIsidFdbIsidId	1.3.6.1.4.1.2272.1.14.23.1.1
rcBridgeIsidFdbAddress	1.3.6.1.4.1.2272.1.14.23.1.2
rcBridgeIsidFdbStatus	1.3.6.1.4.1.2272.1.14.23.1.3
rcBridgeIsidFdbPort	1.3.6.1.4.1.2272.1.14.23.1.4
rcBridgeIsidFdbPortType	1.3.6.1.4.1.2272.1.14.23.1.5
rcBridgeIsidFdbRemoteMacDestAddr	1.3.6.1.4.1.2272.1.14.23.1.6
rcBridgeIsidFdbRemoteMacBVlanId	1.3.6.1.4.1.2272.1.14.23.1.7
rcBridgeIsidFdbRemoteMacDestSysName	1.3.6.1.4.1.2272.1.14.23.1.8
rcnHaCpuState	1.3.6.1.4.1.2272.1.21.0.35
rcL2RedundancyHaCpuState	1.3.6.1.4.1.2272.1.32.1

Modified MIBs

Object Name	Object OID	Modified in Release
rcIsidServiceType	1.3.6.1.4.1.2272.1.87.2.1.2	6.3