Fabric Engine 9.2 Release Notes

New Features, Improvements, and Known Issues

9039124-00 Rev AA
March 2025

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: https://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/

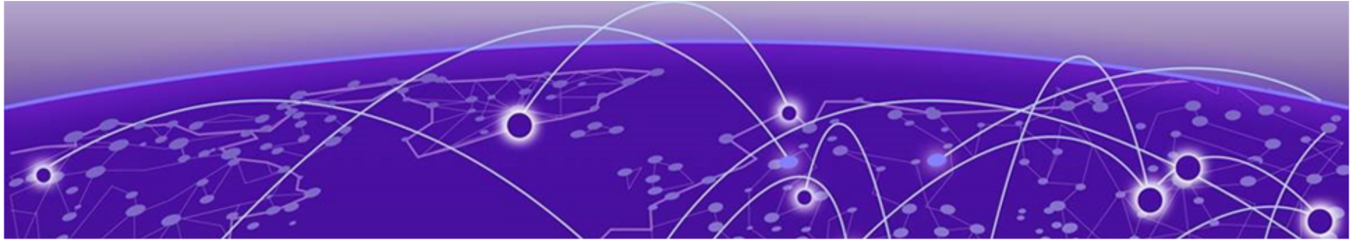


Table of Contents

Abstract...... 6

Preface...... 7

Purpose...... 7

Conventions...... 7

Text Conventions...... 8

Documentation and Training...... 10

Open Source Declarations...... 10

Training...... 10

Help and Support...... 10

Subscribe to Product Announcements...... 11

Send Feedback...... 11

Document Revision Changes...... 13

New in this Release...... 14

New Hardware...... 14

4220 Series...... 14

5320 Series...... 15

New Transceivers and Components...... 16

Managing the 4220 Series...... 16

New Software Features or Enhancements...... 18

Fabric Enhancements...... 18

Operational Enhancements...... 19

Platform Enhancements...... 20

Security Enhancements...... 21

Other Changes...... 21

Scaling Changes...... 21

File Names for this Release...... 21

Upgrade and Downgrade Considerations...... 26

IS-IS Route Tagging...... 27

Validated Upgrade Paths...... 27

Switches That Will Not Use Zero Touch Deployment...... 28

Switches That Will Use Zero Touch Deployment 28

Compatible Fabric IPsec Gateway Versions...... 29

Downgrade Considerations...... 30

ExtremeCloud IQ Agent...... 30

Downgrade ExtremeCloud IQ Managed Switches to 9.0.0.0...... 31

Post Upgrade Configuration for Zero Touch Fabric Configuration and Nickname Assignment...... 31

Network Requirements...... 32

Zero Touch Fabric Configuration Switch...... 33

Hardware and Software Compatibility....36
4220 Series Series Hardware.... 36
5320 Series Hardware....36
5420 Series Hardware....37
5520 Series Hardware....38
Operational Notes....39
Versatile Interface Module Operational Notes.... 39
Operational Notes for VIM Transceivers.... 40
5720 Series Hardware.... 40
Versatile Interface Module Operational Notes.... 41
7520 Series Hardware....41
7520-48YE-8CE Operational Notes.... 41
7720 Series Hardware....41
Transceivers....42
Auto-Negotiation.... 42
Forward Error Correction (FEC)....42
Power Supply Compatibility.... 42

Scaling....44
Layer 2.... 45
Maximum Number of Directed Broadcast Interfaces....51
Maximum Number of Microsoft NLB Cluster IP Interfaces.... 52
IP Unicast.... 52
IP Interface Maximums Clarification....65
IP Interface Maximums for 4220 Series.... 66
IP Interface Maximums for 5320 Series....66
IP Interface Maximums for 5420 Series.... 67
IP Interface Maximums for 5520 Series....67
IP Interface Maximums for 5720 Series.... 68
IP Interface Maximums for 7520 Series.... 68
IP Interface Maximums for 7720 Series.... 69
Layer 3 Route Table Size....70
Route Scaling.... 70
IP Multicast....73
Distributed Virtual Routing (DvR)....78
VXLAN Gateway....80
Filters, QoS, and Security....81
Filter Scaling....85
OAM and Diagnostics....94
Extreme Integrated Application Hosting Scaling....100
Fabric Scaling.... 101
Multi-area SPB Maximums....106
Number of I-SIDs Supported for the Number of Configured IS-IS Interfaces and Adjacencies.... 107
Interoperability Considerations for IS-IS External Metric....110
Recommendations....111
VRF Scaling....111

Important Notices....112
ExtremeCloud IQ Support.... 112

Compatibility with ExtremeCloud IQ Site Engine 112
Licensing 113
Memory Usage 113

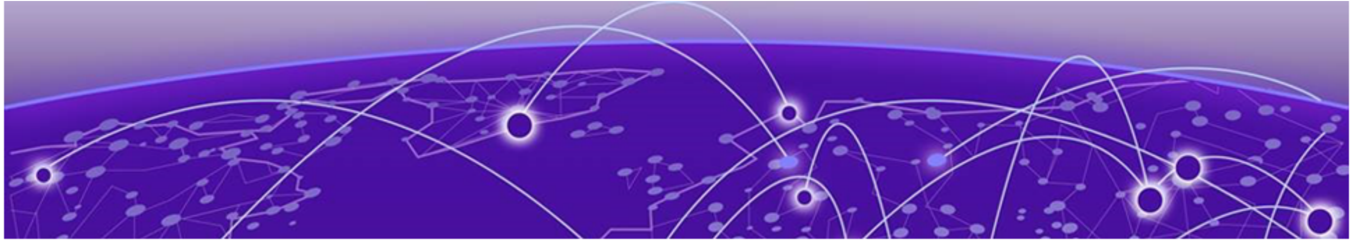
Known Issues and Restrictions 114

Known Issues for this Release 114
Restrictions and Expected Behaviors 126
General Restrictions and Expected Behaviors 127
Filter Restrictions 134

Resolved Issues this Release 136

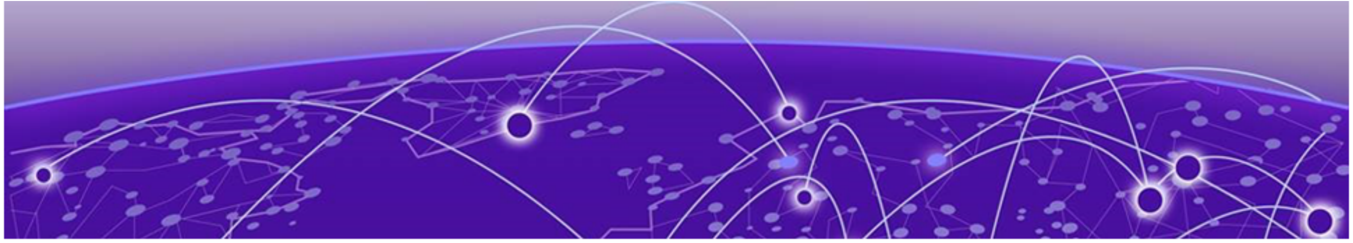
Related Information 138

MIB Changes 138
Deprecated MIBs 138
Modified MIBs 138
New MIBs 146
Obsolete MIBs 156



Abstract

The release notes for Fabric Engine 9.2 provide a comprehensive overview of new features, improvements, and known issues for the platform. Key technical points include enhancements in fabric, operational, platform, and security features. Notable updates include support for new hardware models in the 4220 and 5320 series, as well as new transceivers and components. Fabric enhancements such as Anycast IP Gateway Layer 2 traceroute, increased MAC address limits for Auto-sense, and EAP on Flex UNI ports are detailed. Operational improvements include a CLI command to reset all port parameters, EDM changes, and IPv6 router advertisement options for DNS support. Platform enhancements cover Energy Star certification, subscription licenses, and PoE configuration options. Security updates include modifications to cipher options for SSL/TLS/HTTPS and RADIUS accounting attributes. Scaling changes, upgrade and downgrade considerations, and hardware and software compatibility are addressed. Known issues and restrictions are outlined, along with troubleshooting tips and important configurations for users to be aware of. This release aims to enhance the overall functionality, security, and performance of the Fabric Engine platform.



Preface

Purpose on page 7
Conventions on page 7
Documentation and Training on page 10
Help and Support on page 10
Send Feedback on page 11

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Purpose

This document describes important information about this release for platforms that support Extreme Networks Fabric Engine.

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
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

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.

Table 3: Command syntax (continued)

Convention	Description
	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: • Select **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> <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]`

Table 3: Command syntax (continued)

Convention	Description
Separator (>)	A greater than sign (>) shows separation in menu paths. For example, in the Navigation pane, expand **Configuration** > **Edit**.
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.

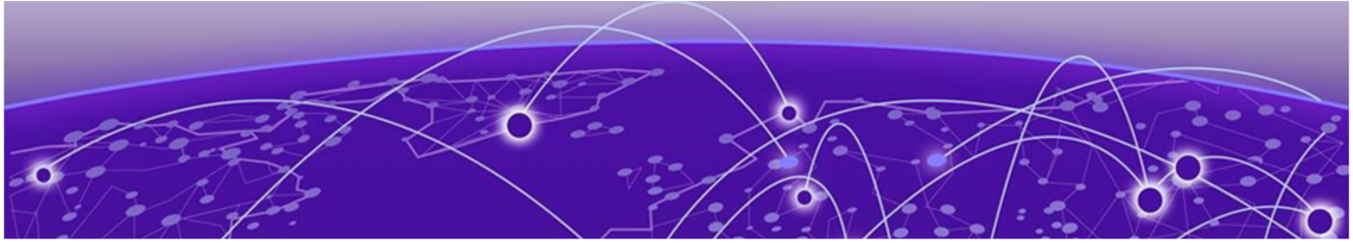
Send Feedback

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 https://www.extremenetworks.com/documentation-feedback/ .

12 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.

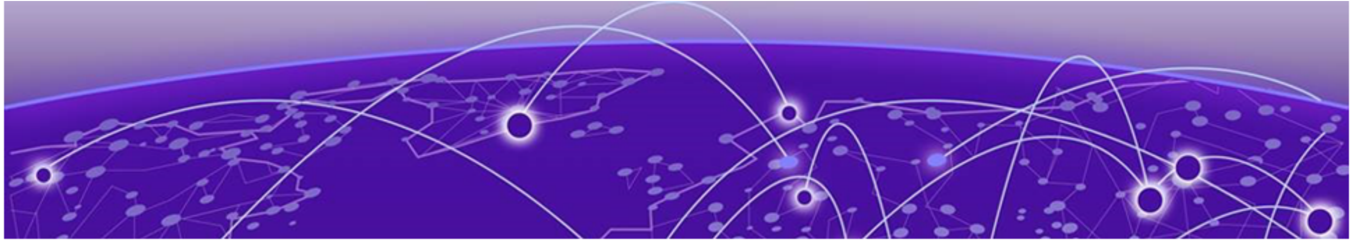


Document Revision Changes

The following table identifies changes between revisions of the same release document.

Table 4: 9.2 Release Notes revision changes

Revision	Change
AA	Initial revision for new release, see New in this Release on page 14



New in this Release

New Hardware on page 14
New Software Features or Enhancements on page 18
Other Changes on page 21
File Names for this Release on page 21

The following platforms support Fabric Engine 9.2:

- ExtremeSwitching 4220 Series
- ExtremeSwitching 5320 Series
- ExtremeSwitching 5420 Series
- ExtremeSwitching 5520 Series
- ExtremeSwitching 5720 Series
- ExtremeSwitching 7520 Series
- ExtremeSwitching 7720 Series

For MIB-related changes, see MIB Changes on page 138.

Note

ExtremeSwitching 5420 Series and 5520 Series: Upgrading from an earlier version of VOSS to Fabric Engine 8.6, or later, on these platforms will change the SNMP SysObjectID value. This change might affect SNMP-based management systems. For more information, see this Knowledge Article.

New Hardware

4220 Series

The 4220 Series are cloud-enabled Layer 2 switches. The 4220 Series maintains all the power and flexibility of a traditional enterprise access switch, while simplifying network operations. Visibility is centralized and Zero-touch provisioning allows rapid deployment across sites. The 4220 Series also provides support for PoE models.

Note

You must apply a Pilot or Extreme Platform ONE license to each switch to obtain access to the full CLI.

This release supports the following 4220 Series models:

- 4220-12P-4X:
  - 12 x 10/100/1000Base-T 802.3at (30W) PoE ports
  - 4 x 1/10Gb SFP+ uplink ports
- 4220-12T-4X:
  - 12 x 10/100/1000Base-T ports
  - 4 x 1/10Gb SFP+ uplink ports
- 4220-24P-4X:
  - 24 x 10/100/1000Base-T 802.3at (30W) PoE ports
  - 4 x 1/10Gb SFP+ uplink ports
- 4220-24T-4X:
  - 24 x 10/100/1000Base-T ports
  - 4 x 1/10Gb SFP+ uplink ports
- 4220-4MW-8P-4X:
  - 8 x 10/100/1000Base-T 802.3at (30W) PoE ports
  - 4 x 1G/2.5G/5GBaseT 802.3bt (90W) PoE ports
  - 4 x 1/10Gb SFP+ uplink ports
- 4220-4MW-20P-4X:
  - 20 x 10/100/1000Base-T 802.3at (30W) PoE ports
  - 4 x 1G/2.5G/5GBaseT 802.3bt (90W) PoE ports
  - 4 x 1/10Gb SFP+ uplink ports
- 4220-8X:
  - 8 x 1/10Gb SFP+ uplink port

In addition to the fixed ports, all 4220 Series models provide one RJ-45 interface port, one Type A USB port, one USB Micro-B console port, and one RJ-45 serial console port.

For optics compatibility, see the Extreme Optics website.

For high-level feature support information, see *Fabric Engine and VOSS Feature Matrix*.

For additional information, see Managing the 4220 Series on page 16.

5320 Series

This release adds support for the following new 5320 Series models:

- 5320-16P-2MXT-2X (not MACsec capable):
  - 16 x 10/100/1000BASE-T full/half duplex, PoE (30w) ports
  - 2 x 10GBASE-T (1G/2.5G/5G/10G capable) uplink ports
  - 2 x 1G/10G SFP+ uplink ports

- 5320-24T-4X-XT (not MACsec capable):
    - 24 x 10/100/1000BASE-T full/half duplex ports

      Note
      The 10/100 ports support half duplex; the 1000 port supports full duplex. Half-duplex is not supported on these ports when operating at 1Gbps.

    - 4 x 1/10Gb SFP+ uplink ports
- 5320-24T-24S-4XE-XT
    - 24 x 10/100/1000BASE-T full/half duplex MACsec capable ports

      Note
      The 10/100 ports support half duplex; the 1000 port supports full duplex. Half-duplex is not supported on these ports when operating at 1Gbps.

    - 4 x 1/10Gb SFP+ MACsec capable uplink ports
    - 24 x 100Mb/1G SFP ports

The 5320-24T-4X-XT and 5320-24T-24S-4XE-XT are extended temperature models in the 5320 Series. These models can function in extended temperatures up to 60°C (32°F), and provide the option to add an external 150W redundant AC power supply. For more information, see *5320 Series Hardware Installation Guide*.

In addition to the fixed ports, these models provide one Type A USB port, one USB Micro-B console port, and one RJ-45 serial console port. 5320-24T-4X-XT and 5320-24T-24S-4XE-XT also provide one RJ-45 interface port.

For optics compatibility, see the Extreme Optics website.

These models support the same feature-based licensing model as other 5320 Series models. For high-level feature support information, see *Fabric Engine and VOSS Feature Matrix*.

New Transceivers and Components

This release introduces support for the following optical devices:

- Optics for 5320-16P-2MXT-2X:
    - 10G ER SFP+ 40km Industrial Temperature (PN:10G-ER-SFP40KM-IT)
    - 10G SR SFP+ 300m Industrial Temperature (PN:10G-SR-SFP300M-IT)
    - 10G LR SFP+ 10km Industrial Temperature (PN:10G-LR-SFP10KM-IT)
    - 100M FX 2KM (PN:100M-FX-SFP2KM-I)

For more information, see the Extreme Optics website.

Managing the 4220 Series

As a cloud-enabled switch, access to configuration commands on 4220 Series differs from earlier switch families. This topic describes those differences.

Full CLI

You can access the full complement of supported CLI commands through the following cloud-management applications:

- Extreme Platform ONE
- ExtremeCloud™ IQ minimum version of 25R2 (S-CLI)
- ExtremeCloud™ IQ Site Engine minimum version of 25.2.10

Note
You must apply a Pilot or Extreme Platform ONE license to each 4220 Series switch to obtain access to the full CLI.

After you use a cloud-management application to enable access to Full CLI, you can use it through direct-switch connection such as the console, Telnet, or SSH. After a Pilot or Extreme Platform ONE license expires, or is revoked, the switch reverts to Basic CLI.

For information about feature support, see *Fabric Engine and VOSS Feature Matrix*.

Basic CLI

You can access a basic CLI directly via the console, Telnet, SSH, or through supported cloud-management applications. Basic CLI is available with the switch Base license and includes all show commands, as well as commands for the following basic configuration, operation, and diagnostic functions:

- boot configuration flags
- certificate management
- clear commands
- DHCP
- diagnostics, such as ping, traceroute, l2ping, l2traceroute, and l2tracetree
- DNS
- Fabric infrastructure—ability to create the Fabric, such as nickname, system ID, Backbone VLAN IDs, and link metric
- IGMP
- IP addressing, Secondary IP Interfaces, default and static routes, and IP interface administrative status
- ExtremeCloud IQ Agent administrative status
- logging and Syslog
- mirroring—port, VLAN, and I-SID
- NTP
- port level attributes, such as Auto-Negotiation, CANA, PoE, jumbo frames, flow control, EEE, and console port configuration
- RADIUS and TACACS+
- Segmented Management Instance
- SNMP
- SPBM configuration script
- STP, MLT, and LAG

- switch operations, such as file system commands, factory default operations, software upgrades, reboots, configuration save and file choices, and system identifying information
- user management
- USB control, if applicable
- VLANs

EDM

By default, EDM is disabled on 4220 Series. Use a supported cloud-management application to enable the web server on the switch. The Full CLI includes the ability to enable the web server.

New Software Features or Enhancements

The following sections describe what is new in this release.

Important
Documentation posted at 9.2 GA includes this document and *Fabric Engine and VOSS Feature Matrix*. Other documentation links in this document refer to 9.1 documents. EDM Help files specific to 9.2 are not available.

Fabric Enhancements

The software supports the following Fabric enhancements:

- Anycast IP Gateway Layer 2 traceroute option—This release extends Layer 2 ping and Layer 2 traceroute to allow you to test connectivity with Anycast IP Gateway I-SIDs.
- Anycast IP Gateway—In this release, Anycast IP Gateway logs messages when you spoof the gateway IP address on an access port of the gateway switch.
- Auto-sense: default changed from 2 to 4 maximum MACs per port—This release increases the maximum number of MAC addresses from 2 to 4. A higher default is useful for network access control (NAC) deployments that have an IP phone with a PC behind it plugged into an Auto-sense port.
- Auto-sense: NNI-AUTH-FAIL state—In this release, ports transition to the NNI-AUTH-FAIL state when a port from a device without an IS-IS Hello Authentication key connects to a port on a device that has an IS-IS Hello Authentication key configured. The NNI-AUTH-FAIL state enables STP multi-homing on the access device while the core switch remains in the NNI-ONBOARDING state to emit fake BPDUs.
- EAP on Flex UNI ports—You can now configure an untagged Switched UNI (S-UNI) on an EAP-enabled interface if one is not already configured. You must associate the untagged S-UNI with a platform VLAN.
- Multi-area SPB: Inter-area duplicate Nickname/System-ID recovery—In this release, Boundary Nodes recover automatically to the full forwarding state after the inter-area duplicate nickname/system ID state is detected.

- **`show khi resource-scaling`** enhancements—This release renames the following Services - IP Multicast fields in the **`show khi resource-scaling`** CLI output:

Previous release	Current release
Multicast local streams	Multicast ingress streams (for those received on UNI)
Multicast remote streams	Multicast egress streams (for those received on NNI)

- Silent devices surviving reboot—The switch stores authenticated client information such as MAC and IP address when the switch reboots. After the switch reboots, it sends regular ARP and ping messages to keep the device authenticated.

Operational Enhancements

The software supports the following operational enhancements:

- CLI command to reset all port parameters to default values—Use the **`default all`** command to configure all port parameters to the default values.

  Note
  After you run the **`default all`** command and you want Auto-sense enabled on the port, use the **`auto-sense enabled`** command.

- EDM changes—This release introduces the following changes:
  - EDM now provides an option to enable or disable counters in the **ACE Common** tab located in **Configuration** > **Security** > **Data Path** > **Advanced Filters (ACE/ ACLs)**.
  - The **802_1ab** folder located in **Serviceability** > **Diagnostics** is renamed to **LLDP & MED**.
  - MACsec and DNS—This release makes the following navigational changes in EDM:

Previous release	Current release
Configuration > **Chassis** > **MACsec**	**Configuration** > **Security** > **Data Path** > **MACsec**
The **DnsDomainName** field is moved from the following location: **Configuration** > **Edit** > **Chassis** > **System**	**Configuration** > **IP** > **DNS** > **Globals**
The **DnsDomainOrigin** and **DNSAdvertisedHostName** fields are moved from the following location: **Configuration** > **Edit** > **Chassis** > **System Flags**	**Configuration** > **IP** > **DNS** > **Globals**

- IPv6 router advertisement options for DNS support—IPv6 Router Advertisement options for DNS (RFC 8106) provide a mechanism for routers to send DNS information using ND messages so the host can acquire DNS configuration dynamically without requiring DHCPv6.

- Network Service Probe—You can create a Network Service Probe interface on a platform VLAN, with or without I-SID, to help troubleshoot network connectivity issues.
- Reduce SLPP-RX reset timer from 6 hours to 300 seconds — In previous releases, SLPP reset the expiry timer every 6 hours, or 21,600 seconds. In this release, SLPP resets the expiry timer every 5 minutes, or 300 seconds.
- **`show lldp neighbor detail`** command updates—The **`show lldp neighbor detail`** command now displays Chassis ID type and Chassis ID information.
- **`show fulltech`** command—You can now only run the **`show full tech`** command in Privileged EXEC mode; you can no longer use it in User EXEC mode.
- SLPP Guard VSA with timers—This release extends the RADIUS SLPP Guard VSA capabilities to enable ports only after a timer expires. The default is 60 seconds.

Platform Enhancements

The software supports the following platform enhancements:

- Energy Star certification—5420 Series, 5520 Series, 5720 Series, and 7520-48XT-6C display the input power and inlet temperature required for Energy Star certification. The **`show sys-info temperature`** command output displays N/A for the temperature value if you do not use a USB thermal sensor.

  Note
  5420F-24S-4XE, 5420F-24T-4XE, and 5420F-48T-4XE are not eligible for Energy Star certification.

- Subscription licenses—If you apply a subscription license to a switch using a cloud-management application, such as Extreme Platform ONE, ExtremeCloud IQ, or ExtremeCloud IQ Site Engine, those applications signal the license to the switch. An Extreme Platform ONE license also enables Premier features on the switch.
- This release automatically creates two archives for logs and message files during the software upgrade process on5420 Series, 5320 Series, and 4220 Series:
  - archive.log.tgz—includes all log* files present in `/intflash/shared`
  - archive.messages.tgz—includes all messages* files present in `/inflash/var/log`

  You can locate the archives in the applicable /inflash folder. All log* files, except for the current one, and all messages* files are deleted.
- PoE—On specific 5420 Series and 5520 Series models, you can configure the PoE Detection Type on a port or range of ports.

  Note
  This change applies to 5420F-48P-4XL, 5420M-16MW-32P-4YE, 5420M-48W-4YE, 5520-24W, and 5520-48W.

- Transceiver support— In addition to supporting 1G full-duplex, the 10070H 10/100/1000BASE-T transceiver extends support to 100M full-duplex on the 5520-48SE.

Security Enhancements

The software supports the following security enhancements:

- EAP 802.1X authentication occurs immediately after the switch receives a CoA Disconnect. In previous releases, the switch waited 30 seconds before starting EAP 802.1X authentication.
- Modifications to cipher options used for SSL/TLS/HTTPS—This release disables the following ciphers for the Web Server:
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

  The **`show web-server`** command displays the updated web server information.
- RADIUS Accounting attribute 8 (Framed-IP-Address)—In this release, the switch uses the Framed-IP-Address RADIUS attribute to export the IPv4 address of an EAP/NEAP client to the RADIUS server. You must enable EAP and Node Alias globally and on an interface.
- RADIUS Message-Authenticator attribute with CoA for EAP and NEAP—The switch can now manage RADIUS requests containing the Message-Authenticator attribute for both EAP or NEAP sessions and includes the Message-Authenticator attribute in all RADIUS authentication requests.

Other Changes

Scaling Changes

All tables are updated to reflect new platforms.

IP Unicast on page 52 is updated to include a note indicating a scaling limitation of 8,000 ARP entries on VLANs without an assigned I-SID on 5520 Series.

Table 25 on page 45 is updated to include the increase to the number of supported MACs with SPBM for 7520 Series and 7720 Series

Multi-area SPB Maximums on page 106 is updated to include the number of supported Multi-area SPB boundary nodes between two areas.

File Names 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 *Fabric Engine User Guide*.

When extracting the software image file, the extraction process appends the software version portion of the extracted file names to include the final full software version. (For example, extracting **`5520.8.2.5.0.voss`** results in a software file named **`5520.8.2.5.0.GA`**.) Ensure that you specify the final full software version (in this case, **`8.2.5.0.GA`**) when using CLI commands that include the software version, such as activating or removing the software.

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

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

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

The following tables provide the file names and sizes for this release.

Table 5: 4220 Series

Description	File	Size
Logs reference	4220.9.2.0.0_edoc.tar	39,823,360 bytes
MD5 Checksum files	4220.9.2.0.0.md5	463 bytes
MIB - supported object names	4220.9.2.0.0_mib_sup.txt	1,446,981 bytes
MIB - objects in the OID compile order	4220.9.2.0.0_mib.txt	8,657,391 bytes
MIB - zip file of all MIBs	4220.9.2.0.0_mib.zip	1,284,277 bytes
Open source software - Master copyright file	4220.9.2.0.0_oss-notice.html	2,889,456 bytes
SHA512 Checksum files	4220.9.2.0.0.sha512	1,378 bytes
Software image	4220.9.2.0.0.voss	114,159,208 bytes
EDM Help files	FabricEnginev9.1.0_HELP_EDM_gzip.zip	5,579,528 bytes
YANG model	restconf_yang.tgz	506,020 bytes

Table 6: 5320 Series Software File names and Sizes

Description	File	Size
Logs reference	5320.9.2.0.0_edoc.tar	39,833,600 bytes
MD5 Checksum files	5320.9.2.0.0.md5	463 bytes
MIB - supported object names	5320.9.2.0.0_mib_sup.txt	1,570,578 bytes
MIB - objects in the OID compile order	5320.9.2.0.0_mib.txt	8,657,391 bytes
MIB - zip file of all MIBs	5320.9.2.0.0_mib.zip	1,284,277 bytes
Open source software - Master copyright file	5320.9.2.0.0_oss-notice.html	2,889,456 bytes

Table 6: 5320 Series Software File names and Sizes (continued)

Description	File	Size
SHA512 Checksum files	5320.9.2.0.0.sha512	1,378 bytes
Software image	5320.9.2.0.0.voss	116,679,265 bytes
EDM Help files	FabricEnginev9.1.0_HELP_EDM_gzip.zip	5,579,528 bytes
YANG model	restconf_yang.tgz	506,020 bytes

Table 7: 5420 Series Software File names and Sizes

Description	File	Size
Logs reference	5420.9.2.0.0_edoc.tar	39,833,600 bytes
MD5 Checksum files	5420.9.2.0.0.md5	463 bytes
MIB - supported object names	5420.9.2.0.0_mib_sup.txt	1,570,344 bytes
MIB - objects in the OID compile order	5420.9.2.0.0_mib.txt	8,657,391 bytes
MIB - zip file of all MIBs	5420.9.2.0.0_mib.zip	1,284,277 bytes
Open source software - Master copyright file	5420.9.2.0.0_oss-notice.html	2,889,456 bytes
SHA512 Checksum files	5420.9.2.0.0.sha512	1,378 bytes
Software image	5420.9.2.0.0.voss	115,967,209 bytes
EDM Help files	FabricEnginev9.1.0_HELP_EDM_gzip.zip	5,579,528 bytes
YANG model	restconf_yang.tgz	506,020 bytes

Table 8: 5520 Series Software File names and Sizes

Description	File	Size
Logs reference	5520.9.2.0.0_edoc.tar	39,833,600 bytes
MD5 Checksum files	5520.9.2.0.0.md5	463 bytes
MIB - supported object names	5520.9.2.0.0_mib_sup.txt	1,569,179 bytes
MIB - objects in the OID compile order	5520.9.2.0.0_mib.txt	8,657,391 bytes
MIB - zip file of all MIBs	5520.9.2.0.0_mib.zip	12,84,277 bytes
Open source software - Master copyright file	5520.9.2.0.0_oss-notice.html	2,889,456 bytes
SHA512 Checksum files	5520.9.2.0.0.sha512	1,378 bytes
Software image	5520.9.2.0.0.voss	127,228,200 bytes

Table 8: 5520 Series Software File names and Sizes (continued)

Description	File	Size
EDM Help files	FabricEnginev9.1.0_HELP_EDM_gzip.zip	5,579,528 bytes
YANG model	restconf_yang.tgz	506,020 bytes

Table 9: 5720 Series Software File names and Sizes

Description	File	Size
Logs reference	5720.9.2.0.0_edoc.tar	39,833,600 bytes
MD5 Checksum files	5720.9.2.0.0.md5	596 bytes
MIB - supported object names	5720.9.2.0.0_mib_sup.txt	1,575,937 bytes
MIB - objects in the OID compile order	5720.9.2.0.0_mib.txt	8,657,391 bytes
MIB - zip file of all MIBs	5720.9.2.0.0_mib.zip	1,284,277 bytes
Open source software - Master copyright file	5720.9.2.0.0_oss-notice.html	2,889,456 bytes
SHA512 Checksum files	5720.9.2.0.0.sha512	1,703 bytes
Software image	5720.9.2.0.0.voss	324,984,024 bytes
EDM Help files	FabricEnginev9.1.0_HELP_EDM_gzip.zip	5,579,528 bytes
Fabric IPsec Gateway	FabricIPSecGW_VM_5.2.0.0.ova	4,034,211,840 bytes
YANG model	restconf_yang.tgz	506,020 bytes
Third Party Virtual Machine (TPVM)	TPVM_Ubuntu20.04_04_14Apr2022.qcow2	4,641,982,464 bytes

Table 10: 7520 Series Software File names and Sizes

Description	File	Size
Logs reference	7520.9.2.0.0_edoc.tar	39,833,600 bytes
MD5 Checksum files	7520.9.2.0.0.md5	596 bytes
MIB - supported object names	7520.9.2.0.0_mib_sup.txt	1,571,930 bytes
MIB - objects in the OID compile order	7520.9.2.0.0_mib.txt	8,657,391 bytes
MIB - zip file of all MIBs	7520.9.2.0.0_mib.zip	1,284,277 bytes
Open source software - Master copyright file	7520.9.2.0.0_oss-notice.html	2,889,456 bytes
SHA512 Checksum files	7520.9.2.0.0.sha512	1,703 bytes
Software image	7520.9.2.0.0.voss	325,283,868 bytes
EDM Help files	FabricEnginev9.1.0_HELP_EDM_gzip.zip	5,579,528 bytes

Table 10: 7520 Series Software File names and Sizes (continued)

Description	File	Size
Fabric IPsec Gateway	FabricIPSecGW_VM_5.2.0.0.ova	4,034,211,840 bytes
YANG model	restconf_yang.tgz	506,020 bytes
Third Party Virtual Machine (TPVM)	TPVM_Ubuntu20.04_04_14Apr2022.qcow2	4,641,982,464 bytes

Table 11: 7720 Series Software File names and Sizes

Description	File	Size
Logs reference	7720.9.2.0.0_edoc.tar	39,833,600 bytes
MD5 Checksum files	7720.9.2.0.0.md5	596 bytes
MIB - supported object names	7720.9.2.0.0_mib_sup.txt	1,570,117 bytes
MIB - objects in the OID compile order	7720.9.2.0.0_mib.txt	8,657,391 bytes
MIB - zip file of all MIBs	7720.9.2.0.0_mib.zip	1,284,277 bytes
Open source software - Master copyright file	7720.9.2.0.0_oss-notice.html	2,889,456 bytes
SHA512 Checksum files	7720.9.2.0.0.sha512	1,703 bytes
Software image	7720.9.2.0.0.voss	325,320,500 bytes
EDM Help files	FabricEnginev9.1.0_HELP_EDM_gzip.zip	5,579,528 bytes
Fabric IPsec Gateway	FabricIPSecGW_VM_5.2.0.0.ova	4,034,211,840 bytes
YANG model	restconf_yang.tgz	506,020 bytes
Third Party Virtual Machine (TPVM)	TPVM_Ubuntu20.04_04_14Apr2022.qcow2	4,641,982,464 bytes

Upgrade and Downgrade Considerations

IS-IS Route Tagging on page 27
Validated Upgrade Paths on page 27
Switches That Will Not Use Zero Touch Deployment on page 28
Switches That Will Use Zero Touch Deployment on page 28
Compatible Fabric IPsec Gateway Versions on page 29
Downgrade Considerations on page 30
Post Upgrade Configuration for Zero Touch Fabric Configuration and Nickname Assignment on page 31

The topics in this section provide information on validated upgrade paths, migration considerations, and compatible software versions.

> **Note**
>
> If a 5420 Series or 5520 Series switch uses DHCP and you did not manually change the host name through the prompt or **`sys name`** command, applications that are hard-coded with the old host name can be impacted after upgrade from a VOSS release to Fabric Engine 8.6 or later. As a workaround, change the system name or prompt back to voss<mac-address>.

See the *Fabric Engine User Guide* for detailed image management procedures that includes information about the following specific upgrade considerations:

- DHCP Server vendor options configuration change
- Considerations for digital certificates

Upgrade switches using one of the options in the following sections:

- Switches That Will Not Use Zero Touch Deployment on page 28
- Switches That Will Use Zero Touch Deployment on page 28

IS-IS Route Tagging

Caution
To use IS-IS Route Tagging on GRT IS-IS routes, you must also configure the metric-type as external. If you want to use IS-IS tags on GRT as internal routes, all Fabric nodes must be above a minimum software version. Any switch in the SPB Fabric that runs earlier software versions triggers an exception if you use metric type internal. To ensure this does not occur, if you attempt to configure a tag and the metric-type is not external, the switch reminds you to upgrade the software on all devices. You must ensure all devices in the network run the minimum required software.

Table 12: Minimum software required

NOS	Minimum software versions
Fabric Engine	8.10.6.1 and later 9.0.5.1 and later 9.1 and later
VOSS	8.10.6.1 and later 9.0.5.1 and later 9.1 and later
VSP 8600 Series	8.1.7 and later

Validated Upgrade Paths

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

Note
For any versions prior to 8.10.0.0, an intermediate upgrade is recommended because pre-8.10.0.0 versions are not validated.
For non-validated upgrade paths, perform the upgrade with one or two switches initially before doing a widespread upgrade.

Table 13: Validated upgrade paths

Product	8.10.x to 9.2	9.0.x to 9.2	9.1.x to 9.2
5320 Series	Y	Y	Y
5420 Series	Y	Y	Y
5520 Series	Y	Y	Y
5720 Series	Y	Y	Y
7520 Series	Y	Y	Y
7720 Series	Y	Y	Y

Switches That Will Not Use Zero Touch Deployment

Switches that will not use Zero Touch Deployment with ExtremeCloud™ IQ or ZTP+ with ExtremeCloud IQ Site Engine should upgrade to this release by performing these steps:

1. Upgrade to this release from one of the previously described releases, see Validated Upgrade Paths on page 27.
2. Continue to use the previous switch configuration.

Switches That Will Use Zero Touch Deployment

Switches that will use Zero Touch Deployment with ExtremeCloud IQ or ZTP+ with ExtremeCloud IQ Site Engine should upgrade to this release by performing the following steps:

Important

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

You do not need to complete this procedure for switches that are already managed by ExtremeCloud IQ or ExtremeCloud IQ Site Engine; use the upgrade functionality available in ExtremeCloud IQ or ExtremeCloud IQ Site Engine.

1. Upgrade to this release from one of the previously described releases, see Validated Upgrade Paths on page 27.
2. Ensure the switch boots without a configuration file. To ensure the switch boots without a configuration file, perform one of the following actions:
   - Rename existing primary and secondary configuration files. Use the **mv** command to rename the existing configuration files. For example, **mv config.cfg config.cfg.backup**.

     This is the preferred option because it ensures that the primary and secondary files are removed while making a backup of them at the same time. This option also ensures that the switch uses the default config.cfg file for the final configuration after it has successfully onboarded.
   - Delete the existing primary and secondary configuration files. Create a backup of these files before you delete them.
   - Boot from non-existent configuration files. Use the **boot config choice** command to configure the primary and backup configuration files to reference files that do not exist on the switch:

     ```
     boot config choice primary config-file nonexistent1.cfg
     ```

     ```
     boot config choice primary backup-config-file nonexistent2.cfg
     ```

     This option also works, however, after the switch has successfully onboarded, it does not use the default config.cfg file but uses the alternative configuration file name provided instead, which might not be desired.
3. Reboot the switch.

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

- The ssh and sshd boot configuration flags are enabled by default.
- All ports are Private VLAN isolated ports.
- VLAN 4048 is created as an *onboarding-vlan* for host-only connectivity for In Band management. All front panel ports are members of VLAN 4048.
- In Band management is enabled.
- Dynamic Host Configuration Protocol (DHCP) client requests are cycled between In Band and Out of Band ports, except on the 5320 Series. 5320 Series supports In Band management only.
- If the switch resets after the IP address is obtained from the DHCP Server, the entire DHCP process does not need to be repeated. Instead, the switch can directly send the DHCP Request to the DHCP Server for the IP stored in the /intflash/dhcp/dhclient.leases file.
- Out of Band management is enabled, except on the 5320 Series. 5320 Series supports In Band management only.
- All ports are administratively enabled.
- IQAgent is enabled by default.
- Zero Touch Provisioning Plus (ZTP+) for ExtremeCloud IQ Site Engine onboarding is enabled by default.
- Zero Touch Fabric Configuration is initiated.
- After the Zero Touch Fabric establishes successfully, the onboarding VLAN 4048 is automatically assigned to onboarding I-SID 15999999.

After the switch reboots in the Zero Touch Deployment configuration, the DHCP client and ExtremeCloud IQ Agent are enabled. The DHCP client obtains an IP address for the switch, DNS discovery is used to discover a Domain Name Server, and the switch attempts to connect to ExtremeCloud IQ and ExtremeCloud IQ Site Engine.

All switches also receive a Zero Touch Fabric Configuration. For more information, see *Fabric Engine User Guide*.

Compatible Fabric IPsec Gateway Versions

> **Note**
> This section only applies to 5720-24MXW, 5720-48MXW, 7520 Series, and 7720 Series. For more information about feature support, see *Fabric Engine and VOSS Feature Matrix*.

The OVA image for the Fabric IPsec Gateway is posted with the image file for each network operating system (NOS) release.

For more information about image files in this release, see File Names for this Release on page 21. For virtual service upgrade instructions, see *Fabric Engine User Guide*.

Only use the Fabric IPsec Gateway image version that is posted with the NOS release image.

Note

Upgrade the switch software image before you upgrade the Fabric IPsec Gateway image.

Downgrade Considerations

Save a backup copy of your switch configuration before upgrading to new release. New releases contain significant enhancements, which cannot be used in previous software versions. Downgrading to an earlier release will require a compatible configuration file.

Caution

If you need to downgrade the image on ExtremeCloud IQ Managed Switches to release 9.0.0.0, from 9.0.2.0, or later, you must remove the file `.telegraf.csv` from the `/intflash` directory if it exists. Failure to do so can cause the switch to crash and revert to 9.0.2.0. For more information, see Downgrade ExtremeCloud IQ Managed Switches to 9.0.0.0 on page 31.

ExtremeCloud IQ Agent

For devices running VOSS 8.3, Fabric Engine 8.6, or later, that connect to ExtremeCloud IQ using ExtremeCloud IQ Agent versions 0.4.0 or higher, you cannot downgrade to VOSS 8.2.x and connect to the cloud automatically. After you downgrade to VOSS 8.2.x, you lose connectivity to ExtremeCloud IQ so you must install a VOSS 8.2.x compatible ExtremeCloud IQ Agent version to re-establish connectivity.

Contact support for assistance with installation of the VOSS 8.2.x compatible ExtremeCloud IQ Agent version. For the support phone number in your country, visit: www.extremenetworks.com/support/contact.

Note

Prior to Fabric Engine 8.6, 5520 Series and 5420 Series platforms ran VOSS. VOSS support ends for these platforms with VOSS 8.5.x.

For information about how to reinstall ExtremeCloud IQ Agent firmware, see *Fabric Engine User Guide*.

Downgrade ExtremeCloud IQ Managed Switches to 9.0.0.0

Perform this procedure to downgrade switches that run GA version 9.0.2.0, or later, and are onboarded using ExtremeCloud IQ. This procedure does not apply to switches onboarded using ExtremeCloud IQ Site Engine.

Before You Begin

This procedure assumes the 9.0.0.0 GA image version is available on the switch. If not, you must upload it and extract the release distribution files to the `/intflash/release/` directory.

Procedure

1. Connect to the switch through the console, SSH, or Telnet.
2. Activate the 9.0.0.0 image:

   ```
   enable

   software activate 9.0.0.0 GA
   ```
3. Disable ExtremeCloud IQ Agent:

   ```
   configure terminal

   application

   no iqagent enable
   ```
4. Delete the following file from the switch:

   ```
   delete /intflash/.telegraf.csv -y
   ```
5. (Optional) Retain a copy of the current configuration, if needed:

   ```
   copy config.cfg config.backup
   ```
6. Ensure the boot configuration points to the saved configuration from 9.0.0.0:

   ```
   copy config.9.0.0.0 config.cfg

   boot config choice primary config-file config.cfg
   ```
7. Reboot the switch to initiate the downgrade:

   ```
   reset -y
   ```
8. Reconnect to the switch and commit the software:

   ```
   enable

   software commit
   ```

Post Upgrade Configuration for Zero Touch Fabric Configuration and Nickname Assignment

Note
In this section, a Zero Touch Fabric release refers to any of the following: VOSS 8.3, Fabric Engine 8.6, or later releases.

The switch initiates Zero Touch Fabric Configuration if you boot without a configuration file.

For Fabric Engine 8.9, or earlier, to add new Zero Touch Fabric Configuration devices or implement Zero Touch Fabric Configuration on existing devices, the network requires a nickname server and reachability to the DHCP server and, optionally, ExtremeCloud IQ servers or ExtremeCloud IQ Site Engine. How you implement Zero Touch Fabric Configuration depends on if the network is a new deployment, or an existing Fabric network that you upgrade. In a new deployment, you can meet the network requirements with one node, known as a seed node. In an existing network, functions can already exist on different nodes.

For devices running Fabric Engine 8.10 or later, the nickname automatically generates when you add new Zero Touch Fabric Configuration devices or implement Zero Touch Fabric Configuration on existing devices. You can configure a nickname server in your network with a dynamic nickname to replace the self-assigned nickname on your device.

For more details on Zero Touch Fabric Configuration, see *Fabric Engine User Guide*.

Important

Not all upgrade paths are validated by Extreme Networks for each new software release. To understand the validated upgrade paths, see Validated Upgrade Paths on page 27.

Network Requirements

The following list identifies the network requirements before you add new Zero Touch Fabric Configuration devices or implement Zero Touch Fabric Configuration on existing devices:

- For devices running releases earlier than Fabric Engine 8.10, you must configure a node as the nickname server, if one does not already exist. This node can be anywhere in the SPB Fabric IS-IS area.
- The DHCP server must be reachable by the remote nodes:
    - In an existing network, the DHCP server can be anywhere in the network. If the DHCP server is on a different IP subnet from the onboarding I-SID, configure DHCP Relay functionality on the existing IP interface of VLAN 4048 with I-SID 15999999.
    - If the DHCP server is on the same subnet as the onboarding I-SID, configure the port facing the DHCP server as private-vlan promiscuous, using Private VLAN 4048, if the new DHCP snooping port feature does not have the promiscuous port configured automatically. This VLAN and the Auto-sense onboarding I-SID are created automatically on a newly deployed device.
- In this release, ports send Fabric Connect LLDP TLVs regardless of the Auto-sense configuration, which means these devices can establish adjacencies with other devices that run a Zero Touch Fabric release, and use either Auto-sense or static NNI configuration.

  In an existing network that includes devices that run a version of VOSS earlier than 8.3, you must manually configure the NNI. Because the port running in the earlier release does not send Fabric Connect LLDP TLVs, an adjacency with a Zero Touch Fabric release node does not form automatically.

For Zero Touch Fabric Configuration to work when a new switch that runs a Zero Touch Fabric release, connects to a switch on an existing Fabric, upgrade at least the existing Fabric switches to a Zero Touch Fabric release first.

- Some SPB deployments use Ethertype 0x88a8 but many use 0x8100. Zero Touch Fabric Configuration works with existing networks that use either value as long as the existing switches that connect to the new switches run a Zero Touch Fabric release.

Zero Touch Fabric Configuration Switch

Important

If you deploy a Fabric-capable switch with Auto-sense enabled, the switch interacts with existing switches that support Fabric Attach (FA). If an existing FA Proxy switch does not have FA server connectivity established yet, it will form an FA connectivity to the newly connected VOSS (8.3 or later) or Fabric Engine, switch as it announces itself as an FA server. To avoid unintended FA connectivity, disable Auto-sense using the **`no auto-sense enable`** command on the relevant ports.

On switches (upgraded existing or newly deployed) where you want to initiate Zero Touch Fabric Configuration, perform the following tasks:

1. Upgrade to a Zero Touch Fabric release, if the device is not a new deployment already running a Zero Touch Fabric release. As a best practice, upgrade to a Fabric Engine release. For a new deployment of universal hardware, ensure the network operating system (NOS) is Fabric Engine.
2. On upgraded existing switches, ensure the switch boots without a configuration file. The switch joins the network as an end host. To ensure the switch boots without a configuration file, perform one of the following actions:
   - Rename existing primary and secondary configuration files. Use the **`mv`** command to rename the existing configuration files. For example, **`mv config.cfg config.cfg.backup`**.

     This is the preferred option because it ensures that the primary and secondary files are removed while making a backup of them at the same time. This option also ensures that the switch uses the default config.cfg file for the final configuration after it has successfully onboarded.
   - Delete the existing primary and secondary configuration files. Create a backup of these files before you delete them.
   - Boot from non-existent configuration files. Use the **`boot config choice`** command to configure the primary and backup configuration files to reference files that do not exist on the switch:

     ```
     boot config choice primary config-file nonexistent1.cfg
     ```

```
boot config choice primary backup-config-file nonexistent2.cfg
```

This option also works, however, after the switch has successfully onboarded, it does not use the default config.cfg file but uses the alternative configuration file name provided instead, which might not be desired.

3. The switch creates a Zero Touch Deployment configuration to onboard the switch, including the following Zero Touch Fabric Configuration items:

   Note
   For more details on Zero Touch Deployment, see *Fabric Engine User Guide*.

   - Creates private VLAN 4048.
   - Enables SPBM.
   - Creates SPBM instance 1.
   - Creates default backbone VLANs (B-VLAN) (4051 and 4052).
   - Creates manual area 00.1515.fee1.900d.1515.fee1.900d.

     Note
     The B-VLAN and manual area configuration values are not compulsory. This remote switch can attach to a Fabric core that does not match these values because the Auto-sense functionality dynamically learns the B-VLANs and manual area in use in the Fabric core from the connected seed node using LLDP.

   - Creates the onboarding I-SID 15999999.
   - Assigns the onboarding I-SID to private VLAN 4048 and also includes the management VLAN.

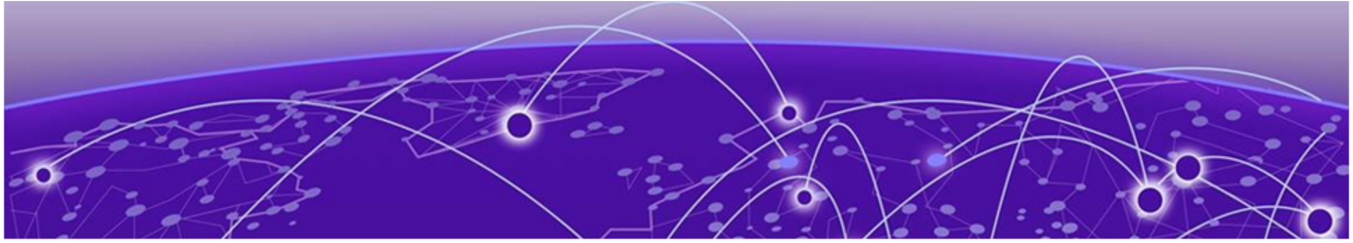
     Note
     As a best practice, use the onboarding I-SID for onboarding purposes and, whenever possible, configure a management VLAN or management CLIP on a different I-SID after the onboarding procedures have been successfully completed.

   - Enables Auto-sense on all ports.
   - Configures Auto-sense access ports and Layer 2 trusted Auto-sense ports.
   - Enables IS-IS globally.
   - With Auto-sense, ports on a switch can detect whether they connect to an SPB device, a Fabric Attach (FA) client, FA Proxy, Voice IP devices, or an undefined host, and then make the necessary configuration.
4. If the seed node uses Auto-sense IS-IS Authentication, configure the remote switch to use the same authentication type and key as the seed node.

   Note
   This step only applies to devices running releases earlier than Fabric Engine 8.10.

5. The switch joins the Fabric.

6. For devices running releases earlier than Fabric Engine 8.10, the nickname server dynamically assigns an SPBM nickname. For devices running releases Fabric Engine 8.10, or later, the switch automatically assigns an SPBM nickname. The device searches the network for a nickname server and if one is found, the device replaces the automatic nickname with the dynamic nickname assigned by the server.
7. After the Zero Touch Fabric establishes successfully, the switch attempts to acquire an IP address on the onboarding VLAN and I-SID using DHCP. When the DHCP client obtains an IP address for the switch, the switch automatically attempts to connect to ExtremeCloud IQ and ExtremeCloud IQ Site Engine.



Hardware and Software Compatibility

4220 Series Series Hardware on page 36
5320 Series Hardware on page 36
5420 Series Hardware on page 37
5520 Series Hardware on page 38
5720 Series Hardware on page 40
7520 Series Hardware on page 41
7720 Series Hardware on page 41
Transceivers on page 42
Power Supply Compatibility on page 42

The topics in this section list the software compatibility for hardware platforms.

4220 Series Series Hardware

4220 Series is a universal hardware product that supports more than one Network Operating System (NOS) personality. For information about NOS personalities, see *Fabric Engine User Guide*.

Table 14: Switch models

Model	Initial Fabric Engine release	Supported new Fabric Engine feature release
		9.2
4220-4MW-8P-4X	9.2	Y
4220-4MW-20P-4X	9.2	Y
4220-8X	9.2	Y
4220-12P-4X	9.2	Y
4220-12T-4X	9.2	Y
4220-24P-4X	9.2	Y
4220-24T-4X	9.2	Y

5320 Series Hardware

5320 Series is a universal hardware product that supports more than one Network Operating System (NOS) personality. For information about NOS personalities, see *Fabric Engine User Guide*.

Table 15: Switch models

Model	Initial Fabric Engine release	Supported new Fabric Engine feature release				
		9.0	9.0.2	9.0.3	9.1	9.2
5320-16P-2MXT-2X	9.2	N	N	N	N	Y
5320-16P-4XE	8.6.1	Y	Y	Y	Y	Y
5320-16P-4XE-DC	8.6.1	Y	Y	Y	Y	Y
5320-24P-8XE	8.6	Y	Y	Y	Y	Y
5320-24T-4X-XT	9.2	N	N	N	N	Y
5320-24T-8XE	8.6	Y	Y	Y	Y	Y
5320-24T-24S-4XE-XT	9.2	N	N	N	N	Y
5320-48P-8XE	8.6	Y	Y	Y	Y	Y
5320-48T-8XE	8.6	Y	Y	Y	Y	Y

5420 Series Hardware

5420 Series is a universal hardware product that supports more than one Network Operating System (NOS) personality. For information about NOS personalities, see *Fabric Engine User Guide*.

Note

Prior to Fabric Engine 8.6, 5420 Series platforms ran VOSS. VOSS support ends for these platforms with VOSS 8.5.x.

Table 16: Switch models

Model	Initial release	Supported new Fabric Engine feature release				
		9.0	9.0.2	9.0.3	9.1	9.2
5420F-8W-16P-4XE	VOSS 8.4	Y	Y	Y	Y	Y
5420F-16W-32P-4XE	VOSS 8.4	Y	Y	Y	Y	Y
5420F-16MW-32P-4XE						
5420F-24S-4XE	VOSS 8.4	Y	Y	Y	Y	Y
5420F-24P-4XE	VOSS 8.4	Y	Y	Y	Y	Y
5420F-24T-4XE	VOSS 8.4	Y	Y	Y	Y	Y
5420F-48P-4XL	VOSS 8.4	Y	Y	Y	Y	Y
5420F-48P-4XE	VOSS 8.4	Y	Y	Y	Y	Y
5420F-48T-4XE	VOSS 8.4	Y	Y	Y	Y	Y
5420M-16MW-32P-4YE	VOSS 8.4	Y	Y	Y	Y	Y
5420M-24T-4YE	VOSS 8.4	Y	Y	Y	Y	Y

Table 16: Switch models (continued)

Model	Initial release	Supported new Fabric Engine feature release				
		9.0	9.0.2	9.0.3	9.1	9.2
5420M-24W-4YE	VOSS 8.4	Y	Y	Y	Y	Y
5420M-48T-4YE	VOSS 8.4	Y	Y	Y	Y	Y
5420M-48W-4YE	VOSS 8.4	Y	Y	Y	Y	Y

5520 Series Hardware

5520 Series is a universal hardware product that supports more than one Network Operating System (NOS) personality. For information about NOS personalities, see *Fabric Engine User Guide*.

Note

Prior to Fabric Engine 8.6, 5520 Series platforms ran VOSS. VOSS support ends for these platforms with VOSS 8.5.x.

Table 17: Switch models

Model	Initial release	Supported new Fabric Engine feature release				
		9.0	9.0.2	9.0.3	9.1	9.2
5520-12MW-36W	VOSS 8.2.5	Y	Y	Y	Y	Y
5520-24T	AC: VOSS 8.2.5	Y	Y	Y	Y	Y
	ACDC: Fabric Engine 9.0					
5520-24W	VOSS 8.2.5	Y	Y	Y	Y	Y
5520-24X	AC: VOSS 8.2.5	Y	Y	Y	Y	Y
	ACDC: Fabric Engine 9.0					
5520-48SE	AC: VOSS 8.2.5	Y	Y	Y	Y	Y
	ACDC: Fabric Engine 9.0					

Table 17: Switch models (continued)

Model	Initial release	Supported new Fabric Engine feature release				
		9.0	9.0.2	9.0.3	9.1	9.2
5520-48T	AC: VOSS 8.2.5	Y	Y	Y	Y	Y
	ACDC: Fabric Engine 9.0					
5520-48W	VOSS 8.2.5	Y	Y	Y	Y	Y

Note

Ensure the switch runs, at a minimum, the noted initial software release before you install a VIM.

Table 18: Versatile Interface Modules (VIMs)

Model	Initial release	Supported new Fabric Engine feature release				
		9.0	9.0.2	9.0.3	9.1	9.2
5520-VIM-4X	VOSS 8.2.5	Y	Y	Y	Y	Y
5520-VIM-4XE	VOSS 8.2.5	Y	Y	Y	Y	Y
5520-VIM-4YE	VOSS 8.2.5	Y	Y	Y	Y	Y

Operational Notes

- The 5520-24T, 5520-24X, 5520-48SE, and 5520-48T models require a minimum of Fabric Engine 8.9 to support power supplies and fans with back-to-front airflow.
- The 5520-24T-ACDC, 5520-24X-ACDC, 5520-48SE-ACDC, and 5520-48T-ACDC models require a minimum of Fabric Engine 9.0 to support DC power supplies.

Versatile Interface Module Operational Notes

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

Table 19: 5520-VIM Matrix

	5520-VIM-4X	5520-VIM-4XE	5520-VIM-4YE
Operational speeds	1Gbps & 10Gbps	1Gbps & 10Gbps	10Gbps & 25Gbps
PHY present	No	Yes	Yes
1000BASE-T & 10GBASE-T	10GBASE-T only	Both	10GBASE-T only
Mixed speeds	1Gbps & 10Gbps	1Gbps & 10Gbps	Mixed speeds not supported
1G Auto-negotiation	Disabled	Disabled	Disabled
10G Auto-negotiation	Disabled	Disabled	Disabled

Table 19: 5520-VIM Matrix (continued)

	5520-VIM-4X	5520-VIM-4XE	5520-VIM-4YE
25G Auto-negotiation			Enabled for DAC Disabled for Fiber
FEC	Not supported	Not supported	Auto-FEC enabled for DAC and Fiber
MACsec	Not supported	128/256 bit	128/256 bit

Operational Notes for VIM Transceivers

The IEEE 802.3by requirement for 25 Gb is that any transceiver or DAC 3 meters or longer, requires the use of forward error correction (FEC).

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

5720 Series Hardware

5720 Series is a universal hardware product that supports more than one Network Operating System (NOS) personality. For information about NOS personalities, see *Fabric Engine User Guide*.

Table 20: Switch models

Model	Initial Fabric Engine release	Supported new feature release				
		9.0	9.0.2	9.0.3	9.1	9.2
5720-24MW	8.7	Y	Y	Y	Y	Y
5720-24MXW	8.7	Y	Y	Y	Y	Y
5720-48MW	8.7	Y	Y	Y	Y	Y
5720-48MXW	8.7	Y	Y	Y	Y	Y

Note

Ensure the switch runs, at a minimum, the noted initial software release before you install a VIM.

Table 21: Versatile Interface Modules (VIMs)

Model	Initial Fabric Engine release	Supported new feature release				
		9.0	9.0.2	9.0.3	9.1	9.2
5720-VIM-2CE	8.7	Y	Y	Y	Y	Y
5720-VIM-6YE	8.7	Y	Y	Y	Y	Y

Versatile Interface Module Operational Notes

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

Table 22: 5720-VIM Matrix

	5720-VIM-2CE	5720-VIM-6YE
Operational speeds	10/25/40/100Gbps	1/10/25Gbps
PHY present	Yes	Yes
1000BASE-T & 10GBASE-T	10GBASE-T only	Both
Mixed speeds	10/25/40Gbps	1/10/25Gbps
1G Auto-negotiation	Not supported	Not supported
10G Auto-negotiation	Not supported	Not supported
25G Auto-negotiation	Supported	Supported
FEC	Supports CL74/CL91	Supports CL74/CL91
MACsec	128/256 bit	128/256 bit

7520 Series Hardware

7520 Series is a universal hardware product that supports more than one Network Operating System (NOS) personality. For information about NOS personalities, see *7520 Series Hardware Installation Guide*.

Table 23: Switch models

Model	Initial Fabric Engine release	Supported new Fabric Engine feature release				
		9.0	9.0.2	9.0.3	9.1	9.2
7520-48Y-8C	8.10	Y	Y	Y	Y	Y
7520-48YE-8CE	9.0	Y	Y	Y	Y	Y
7520-48XT-6C	8.10	Y	Y	Y	Y	Y

7520-48YE-8CE Operational Notes

7520-48YE-8CE does not support 1/25Gbps optics or DACs.

7720 Series Hardware

7720 Series is a universal hardware product that supports more than one Network Operating System (NOS) personality. For information about NOS personalities, see *7720 Series Hardware Installation Guide*.

Table 24: Switch models

Model	Initial Fabric Engine release	Supported new Fabric Engine feature release				
		9.0	9.0.2	9.0.3	9.1	9.2
7720-32C	8.10	Y	Y	Y	Y	Y

Transceivers

The software allows the use of transceivers and direct attach cables from any vendor, which means that the switch will bring up the port operationally when using any transceiver. Extreme Networks does not provide support for operational issues related to the use of non-Extreme Networks branded transceivers and direct attached cables used in the switches.

To find product descriptions and compatibility information for optical transceivers and components, visit the Extreme Optics website.

Auto-Negotiation

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

When you use a 1 Gb SFP transceiver on a 10 Gb SFP+ port, ensure that auto-negotiation is enabled.

For 1000BASE-T SFP transceivers, the best practice is to perform custom auto-negotiation at the remote native copper port. This can prevent connections from failing if the speed or duplex negotiation changes.

Forward Error Correction (FEC)

Forward Error Correction (FEC) is a method of obtaining error control in data transmission over an unreliable or noisy channel in which the source (transmitter) encodes the data in a redundant way by using an error correcting code (ECC). This redundancy enables a destination (receiver) to detect a limited number of errors and correct them without requiring a re-transmission.

For more information about FEC, see *Fabric Engine User Guide*.

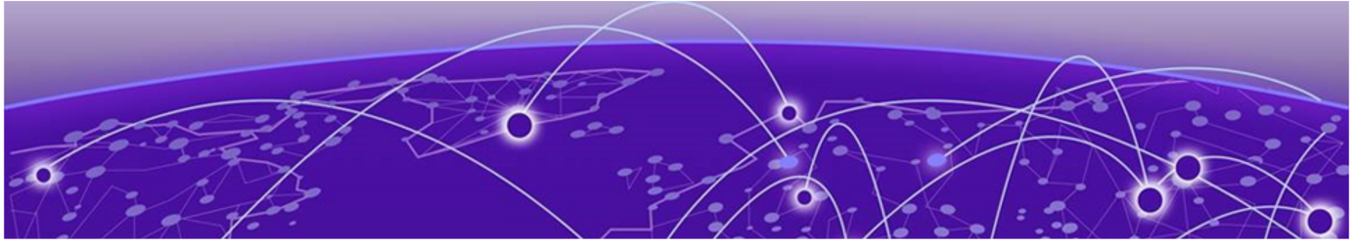
Power Supply Compatibility

You can use certain power supplies in more than one platform.

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

- *4220 Series Hardware Installation Guide*
- *5320 Series Hardware Installation Guide*

- *5420 Series Hardware Installation Guide*
- *5520 Series Hardware Installation Guide*
- *5720 Series Hardware Installation Guide*
- *7520 Series Hardware Installation Guide*
- *7720 Series Hardware Installation Guide*



Scaling

Layer 2 on page 45
IP Unicast on page 52
Layer 3 Route Table Size on page 70
IP Multicast on page 73
Distributed Virtual Routing (DvR) on page 78
VXLAN Gateway on page 80
Filters, QoS, and Security on page 81
OAM and Diagnostics on page 94
Extreme Integrated Application Hosting Scaling on page 100
Fabric Scaling on page 101
VRF Scaling on page 111

This section documents scaling capabilities of the universal hardware platforms.

Note
Feature support can differ within a product family. Scaling numbers for a product family do not always reflect when a feature is not supported on a specific model. For feature support information, see *Fabric Engine and VOSS Feature Matrix*.

The scaling and performance information shown in the following tables is provided for the purpose of assisting with network design. It is recommended that network architects and administrators design and manage networks with an appropriate level of network scaling “head room.” The scaling and performance figures provided have been verified using specific network topologies using limited switch configurations. There is no guarantee that the scaling and performance figures shown are applicable to all network topologies and switch configurations and are provided as a realistic estimation only. If you experience scaling and performance characteristics that you feel are sufficiently below what has been documented, contact Extreme Networks technical support for additional assistance.

Note

If your switch uses Advanced Feature Bandwidth Reservation in Full Feature mode, this affects scaling information that is based on the number of available ports. If you enable the boot configuration flag for this feature, remember to deduct the number of reserved ports from the documented scaling maximum. Not all hardware platforms require this feature to provide full feature support. For more information, see *Fabric Engine User Guide*.

Layer 2

Table 25: Layer 2 Maximums

Attribute	Product	Maximum number supported
MAC table size (without SPBM)	4220 Series	32,000
	5320 Series	32,000
	5420 Series	5420F Series models: 32,000 5420M Series models: 64,000
	5520 Series	80,000
	5720 Series	5720MXW models: 164,000 5720MW models: 100,000
	7520 Series	160,000
	7720 Series	160,000
MAC table size (with SPBM)	4220 Series	16,000
	5320 Series	16,000
	5420 Series	5420F Series models: 16,000 5420M Series models: 32,000
	5520 Series	40,960
	5720 Series	5720MXW models: 82,000 5720MW models: 50,000
	7520 Series	120,000
	7720 Series	120,000
Endpoint Tracking MAC addresses per switch	4220 Series	n/a
	5320 Series	n/a
	5420 Series	n/a
	5520 Series	8,000
	5720 Series	8,000
	7520 Series	8,000
	7720 Series	8,000

Table 25: Layer 2 Maximums (continued)

Attribute	Product	Maximum number supported
Directed Broadcast interfaces	4220 Series	100 See Maximum Number of Directed Broadcast Interfaces on page 51.
	5320 Series	200 See Maximum Number of Directed Broadcast Interfaces on page 51.
	5420 Series	200 See Maximum Number of Directed Broadcast Interfaces on page 51.
	5520 Series	200 See Maximum Number of Directed Broadcast Interfaces on page 51.
	5720 Series	200 See Maximum Number of Directed Broadcast Interfaces on page 51.
	7520 Series	200 See Maximum Number of Directed Broadcast Interfaces on page 51.
	7720 Series	200 See Maximum Number of Directed Broadcast Interfaces on page 51.
Port-based VLANs Note: When you use Flex-UNI functionality, you can use the range from 1 to 4094 for port VLAN IDs.	4220 Series	4,059
	5320 Series	4,059
	5420 Series	4,059
	5520 Series	4,059
	5720 Series	4,059
	7520 Series	4,059
	7720 Series	4,059

Table 25: Layer 2 Maximums (continued)

Attribute	Product	Maximum number supported
Private VLANs	4220 Series	See Table 26 on page 51
	5320 Series	See Table 26 on page 51
	5420 Series	See Table 26 on page 51
	5520 Series	See Table 26 on page 51
	5720 Series	See Table 26 on page 51
	7520 Series	See Table 26 on page 51
	7720 Series	See Table 26 on page 51
Protocol-based VLANs (IPv6 only)	4220 Series	n/a
	5320 Series	1
	5420 Series	1
	5520 Series	1
	5720 Series	1
	7520 Series	1
	7720 Series	1
RSTP instances	4220 Series	1
	5320 Series	1
	5420 Series	1
	5520 Series	1
	5720 Series	1
	7520 Series	1
	7720 Series	1
MSTP instances	4220 Series	12
	5320 Series	12
	5420 Series	12
	5520 Series	12
	5720 Series	12
	7520 Series	12
	7720 Series	12

Table 25: Layer 2 Maximums (continued)

Attribute	Product	Maximum number supported
LACP aggregators	4220 Series	28
	5320 Series	48-port models: 56 5320-24T-4X-XT: 28 Other 24-port models: 32 5320-16P-4XE: 20 5320-16P-2MXT-2X: 16
	5420 Series	56 (48 fixed ports, 4 Universal Ethernet ports, 4 SFP-DD ports)
	5520 Series	48-port models: up to 60 with channelization 24-port models: up to 36 with channelization
	5720 Series	64
	7520 Series	56
	7720 Series	32 (up to 125 with channelization)
Ports per LACP aggregator	4220 Series	8 active
	5320 Series	8 active
	5420 Series	8 active
	5520 Series	8 active
	5720 Series	8 active
	7520 Series	8 active
	7720 Series	8 active
MLT groups	4220 Series	28
	5320 Series	48-port models: 56 5320-24T-4X-XT: 28 Other 24-port models: 32 5320-16P-4XE: 20 5320-16P-2MXT-2X: 16
	5420 Series	56 (48 fixed ports, 4 Universal Ethernet ports, 4 SFP-DD ports)
	5520 Series	48-port models: up to 60 with channelization 24-port models: up to 36 with channelization
	5720 Series	64
	7520 Series	56
	7720 Series	32 (up to 125 with channelization)

Table 25: Layer 2 Maximums (continued)

Attribute	Product	Maximum number supported
Ports per MLT group	4220 Series	8 active
	5320 Series	8 active
	5420 Series	8 active
	5520 Series	8
	5720 Series	8
	7520 Series	8
	7720 Series	8
Link State Tracking (LST) groups	4220 Series	48
	5320 Series	48
	5420 Series	48
	5520 Series	48
	5720 Series	48
	7520 Series	48
	7720 Series	48
Interfaces per LST group	4220 Series	8 upstream/28 downstream
	5320 Series	48-port models: 9 upstream/128 downstream 5320-24T-4X-XT: 8 upstream/28 downstream 16- and other 24-port models: 8 upstream/128 downstream
	5420 Series	8 upstream 128 downstream
	5520 Series	8 upstream 128 downstream
	5720 Series	8 upstream 128 downstream
	7520 Series	8 upstream 128 downstream
	7720 Series	8 upstream 128 downstream

Table 25: Layer 2 Maximums (continued)

Attribute	Product	Maximum number supported
SLPP VLANs	4220 Series	64
	5320 Series	128
	5420 Series	128
	5520 Series	128
	5720 Series	500
	7520 Series	500
	7720 Series	500
VLACP interfaces	4220 Series	28
	5320 Series	48-port models: 56 5320-24T-4X-XT: 28 Other 24-port models: 32 5320-16P-4XE: 20 5320-16P-2MXT-2X: 16
	5420 Series	56 (48 fixed ports, 4 Universal Ethernet ports, 4 SFP-DD ports)
	5520 Series	48-port models: up to 60 with channelization 24-port models: up to 36 with channelization
	5720 Series	64 with no SPB mode: up to 56 with SPBM mode with the channelization enabled when using 5720-VIM-2CE. 64 with no VIM: up to 54 with 5720-VIM-6YE.
	7520 Series	56
	7720 Series	32 (up to 125 with channelization)

Table 25: Layer 2 Maximums (continued)

Attribute	Product	Maximum number supported
Microsoft NLB cluster IP interfaces	4220 Series	Not supported
	5320 Series	Not supported
	5420 Series	Not supported
	5520 Series	200 See Maximum Number of Microsoft NLB Cluster IP Interfaces on page 52.
	5720 Series	200 See Maximum Number of Microsoft NLB Cluster IP Interfaces on page 52.
	7520 Series	200 See Maximum Number of Microsoft NLB Cluster IP Interfaces on page 52.
	7720 Series	200 See Maximum Number of Microsoft NLB Cluster IP Interfaces on page 52.

The number of Private VLANs/Layer 2 E-Tree varies depending on the number of private VLAN trunk ports as members. The following table provides the maximum numbers.

Table 26: Private VLAN and Layer 2 E-Tree maximums

Platform	Total Private VLANs and Layer 2 E-Tree with 2 Private VLAN trunk ports	Total Private VLANs and Layer 2 E-Tree with 4 Private VLAN trunk ports
4220 Series	5	5
5320 16- and 24-port models	40	20
5320 48-port models	100	50
5420 Series	100	50
5520 Series	200	100
5720 Series	200	100
7520 Series	100	50
7720 Series	100	50

Maximum Number of Directed Broadcast Interfaces

The number of Directed Broadcast interfaces must be less than or equal to 200. However, if you configure VLANs with both NLB and Directed Broadcast, you can only scale up to 100 VLANs.

Maximum Number of Microsoft NLB Cluster IP Interfaces

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

For example: 1 virtual interface per cluster x 200 clusters = 200 or 2 virtual interfaces per cluster x 100 clusters = 200

However, if you configure VLANs with both NLB and Directed Broadcast, you can only scale up to 100 VLANs assuming there is only 1 NLB cluster IP interface per VLAN.

IP Unicast

Table 27: IP Unicast Maximums

Attribute	Product	Maximum number supported
IP interfaces (IPv4 or IPv6 or IPv4+IPv6)	4220 Series	128 See IP Interface Maximums for 4220 Series on page 66.
	5320 Series	248 See IP Interface Maximums for 5320 Series on page 66.
	5420 Series	248 See IP Interface Maximums for 5420 Series on page 67.
	5520 Series	500 See IP Interface Maximums for 5520 Series on page 67.
	5720 Series	1,000 See IP Interface Maximums for 5720 Series on page 68.
	7520 Series	1,000 See IP Interface Maximums for 7520 Series on page 68
	7720 Series	1,000 See IP Interface Maximums for 7720 Series on page 69

Table 27: IP Unicast Maximums (continued)

Attribute	Product	Maximum number supported
VRRP interfaces (IPv4 or IPv6)	4220 Series	32 See IP Interface Maximums for 4220 Series on page 66.
	5320 Series	48-port models: 124 16- and 24-port models: 64 See IP Interface Maximums for 5320 Series on page 66.
	5420 Series	124 See IP Interface Maximums for 5420 Series on page 67.
	5520 Series	252 See IP Interface Maximums for 5520 Series on page 67.
	5720 Series	500 See IP Interface Maximums for 5720 Series on page 68.
	7520 Series	500 See IP Interface Maximums for 7520 Series on page 68
	7720 Series	500 See IP Interface Maximums for 7720 Series on page 69

Table 27: IP Unicast Maximums (continued)

Attribute	Product	Maximum number supported
Anycast IP Gateway interfaces	4220 Series	32 See IP Interface Maximums for 4220 Series on page 66
	5320 Series	48-port models: 124 16- and 24-port models: 64 See IP Interface Maximums for 5320 Series on page 66.
	5420 Series	124 See IP Interface Maximums for 5420 Series on page 67.
	5520 Series	252 126 on boundary node See IP Interface Maximums for 5520 Series on page 67.
	5720 Series	500 250 on boundary node See IP Interface Maximums for 5720 Series on page 68.
	7520 Series	500 250 on boundary node See IP Interface Maximums for 7520 Series on page 68
	7720 Series	500 250 on boundary node See IP Interface Maximums for 7720 Series on page 69

Table 27: IP Unicast Maximums (continued)

Attribute	Product	Maximum number supported
Routed Split Multi-Link Trunking (RSMLT) interfaces (IPv4 or IPv6 or IPv4+IPv6)	4220 Series	n/a
	5320 Series	n/a
	5420 Series	124 See IP Interface Maximums for 5420 Series on page 67.
	5520 Series	499 See IP Interface Maximums for 5520 Series on page 67.
	5720 Series	500 See IP Interface Maximums for 5720 Series on page 68.
	7520 Series	500 See IP Interface Maximums for 7520 Series on page 68
	7720 Series	500 See IP Interface Maximums for 7720 Series on page 69
VRRP interfaces with fast timers (200ms) - IPv4/IPv6	4220 Series	0
	5320 Series	24
	5420 Series	24
	5520 Series	24
	5720 Series	24 See IP Interface Maximums for 5720 Series on page 68.
	7520 Series	24 See IP Interface Maximums for 7520 Series on page 68
	7720 Series	24 See IP Interface Maximums for 7720 Series on page 69

Table 27: IP Unicast Maximums (continued)

Attribute	Product	Maximum number supported
ECMP groups/paths per group	4220 Series	32/8
	5320 Series	48-port models: 64/8 5320-16P-4XE and 24-port models: 32/8 5320-16P-2MXT-2X: 128/8
	5420 Series	64/8
	5520 Series	256/8
	5720 Series	2,048/8
	7520 Series	2,048/8
	7720 Series	2,048/8
OSPF v2/v3 interfaces	4220 Series	n/a
	5320 Series	48-port models: 50 5320-24T-4X-XT: 8 16- and other 24-port models: 1
	5420 Series	50
	5520 Series	100
	5720 Series	65
	7520 Series	65
	7720 Series	65
OSPF v2/v3 neighbors (adjacencies)	4220 Series	n/a
	5320 Series	50
	5420 Series	50
	5520 Series	100
	5720 Series	500
	7520 Series	500
	7720 Series	500

Table 27: IP Unicast Maximums (continued)

Attribute	Product	Maximum number supported
OSPF areas	4220 Series	n/a
	5320 Series	48-port models: 12 16- and 24-port models: 4
	5420 Series	12 for the switch
	5520 Series	12 for each VRF 80 for the switch
	5720 Series	12 for each VRF 80 for the switch
	7520 Series	12 for each VRF 80 for the switch
	7720 Series	12 for each VRF 80 for the switch
IPv4 ARP table	4220 Series	4,000
	5320 Series	48-port models: 15,000 5320-16P-2MXT-2X and 5320-24T-4X-XT: 4,000 5320-16P-4XE and other 24-port models: 8,000
	5420 Series	5420F Series models: 15,000 5420M Series models: 24,000
	5520 Series	16,000 **Note:** There is a scaling limitation of 8,000 ARP entries on VLANs without an assigned I-SID. For more information, see VOSS-32270 in Known Issues for this Release on page 114.
	5720 Series	5720MW Series models: 24,000 5720MXW Series models: 64,000
	7520 Series	40,000 with SPB
	7720 Series	40,000 with SPB
IPv4 CLIP interfaces	4220 Series	16
	5320 Series	64
	5420 Series	64
	5520 Series	64
	5720 Series	64
	7520 Series	64
	7720 Series	64

Table 27: IP Unicast Maximums (continued)

Attribute	Product	Maximum number supported
IPv4 RIP interfaces	4220 Series	n/a
	5320 Series	50
	5420 Series	50
	5520 Series	100
	5720 Series	200
	7520 Series	200
	7720 Series	200
IPv4 BGP peers	4220 Series	n/a
	5320 Series	8
	5420 Series	8
	5520 Series	16
	5720 Series	256
	7520 Series	256
	7720 Series	256
IPv4 VRFs with iBGP	4220 Series	n/a
	5320 Series	5320-16P-2MXT-2X, 5320-24T-4X-XT, and 48-port models: 8 5320-16P-4XE and other 24-port models: 1
	5420 Series	8
	5520 Series	16
	5720 Series	16
	7520 Series	16
	7720 Series	16

Table 27: IP Unicast Maximums (continued)

Attribute	Product	Maximum number supported
IPv4/IPv6 VRF instances For additional information, see VRF Scaling on page 111.	4220 Series	1
	5320 Series	48-port models: 64 5320-16P-2MXT-2X and 5320-24T-4X-XT: 8 5320-16P-4XE and other 24-port models: 1 See IP Interface Maximums for 5320 Series on page 66.
	5420 Series	64 See IP Interface Maximums for 5420 Series on page 67.
	5520 Series	256 including mgmt VRF and GRT See IP Interface Maximums for 5520 Series on page 67.
	5720 Series	256 See IP Interface Maximums for 5720 Series on page 68.
	7520 Series	256 See IP Interface Maximums for 7520 Series on page 68
	Note: 7720 Series	256 See IP Interface Maximums for 7720 Series on page 69
IPv4 static ARP entries	4220 Series	1,000 per switch
	5320 Series	48-port models: 1,000 per VRF/ 5,000 per switch 16- and 24-port models: 1,000 per switch
	5420 Series	1,000 per VRF 5,000 per switch
	5520 Series	2,000 for each VRF 10,000 for the switch
	5720 Series	2,000 for each VRF 10,000 for the switch
	7520 Series	2,000 for each VRF 10,000 for the switch
	7720 Series	2,000 for each VRF 10,000 for the switch

Table 27: IP Unicast Maximums (continued)

Attribute	Product	Maximum number supported
IPv4 static routes	4220 Series	500 per switch
	5320 Series	48-port models: 500 per VRF/ 2,500 per switch 16- and 24-port models: 500 per switch
	5420 Series	500 per VRF 2500 per switch
	5520 Series	1,000 for each VRF 5,000 for the switch
	5720 Series	1,000 for each VRF 5,000 for the switch
	7520 Series	1,000 for each VRF 5,000 for the switch
	7720 Series	1,000 for each VRF 5,000 for the switch
IPv4 route policies	4220 Series	n/a
	5320 Series	5320-24T-4X-XT and 48-port models: 50 per VRF/500 per switch 16- and other 24-port models: 500 per switch
	5420 Series	50 per VRF 500 per switch
	5520 Series	500 for each VRF 5,000 for the switch
	5720 Series	500 for each VRF 5,000 for the switch
	7520 Series	500 for each VRF 5,000 for the switch
	7720 Series	500 for each VRF 5,000 for the switch
IPv4 UDP forwarding entries	4220 Series	128
	5320 Series	128
	5420 Series	128
	5520 Series	256
	5720 Series	512
	7520 Series	1,024
	7720 Series	1,024

Table 27: IP Unicast Maximums (continued)

Attribute	Product	Maximum number supported
DHCP client addresses provided by the DHCP server	4220 Series	1,000 clients
	5320 Series	1,000 clients
	5420 Series	10,000 clients
	5520 Series	10,000 clients
	5720 Series	100,000 clients
	7520 Series	100,000 clients
	7720 Series	100,000 clients
IPv4 DHCP Relay forwarding entries	4220 Series	128
	5320 Series	248
	5420 Series	248
	5520 Series	512
	5720 Series	2,048
	7520 Series	2,048
	7720 Series	2,048
IPv6 DHCP Snoop entries in Source Binding Table	4220 Series	512
	5320 Series	512
	5420 Series	512
	5520 Series	1,024
	5720 Series	1,024
	7520 Series	1,024
	7720 Series	1,024
IPv6 Neighbor table	4220 Series	n/a
	5320 Series	5320-16P-2MXT-2X: 4,000 5320-24T-4X-XT: 2,000 All other models: 8,000
	5420 Series	5420F Series models: 8,000 5420M Series models: 16,000
	5520 Series	16,000
	5720 Series	5720MW Series models: 24,000 5720MXW Series models: 32,000
	7520 Series	32,000
	7720 Series	32,000

Table 27: IP Unicast Maximums (continued)

Attribute	Product	Maximum number supported
IPv6 static entries in Source Binding Table	4220 Series	n/a
	5320 Series	48-port models: 65 per VRF/ 256 per switch 16- and 24-port models: 256 per switch
	5420 Series	64 per VRF 256 per system
	5520 Series	128 per VRF 512 per system
	5720 Series	256
	7520 Series	256
	7720 Series	256
IPv6 static neighbor records	4220 Series	n/a
	5320 Series	5320-24T-4X-XT and 48-port models: 64 per VRF/256 per switch 16- and other 24-port models: 256 per switch
	5420 Series	64 per VRF 256 per switch
	5520 Series	128 per VRF 512 per system
	5720 Series	128 per VRF 512 per system
	7520 Series	128 per VRF 512 per system
	7720 Series	128 per VRF 512 per system
IPv6 CLIP interfaces	4220 Series	1 for mgmt only
	5320 Series	64
	5420 Series	64
	5520 Series	64
	5720 Series	64
	7520 Series	64
	7720 Series	64

Table 27: IP Unicast Maximums (continued)

Attribute	Product	Maximum number supported
IPv6 static routes	4220 Series	n/a
	5320 Series	5320-16P-4XE, 24-port, and 48-port models: 500 5320-16P-2MXT-2X: 128
	5420 Series	500
	5520 Series	1,000
	5720 Series	1,000
	7520 Series	1,000
	7720 Series	1,000
IPv6 6in4 configured tunnels	4220 Series	n/a
	5320 Series	32
	5420 Series	32
	5520 Series	64
	5720 Series	64
	7520 Series	64
	7720 Series	64
IPv6 DHCP Relay forwarding	4220 Series	128
	5320 Series	248
	5420 Series	248
	5520 Series	256 per switch 10 per VRF
	5720 Series	512 per switch 10 per VRF
	7520 Series	512 per switch
	7720 Series	512 per switch
IPv6 BGP peers	4220 Series	n/a
	5320 Series	8
	5420 Series	8
	5520 Series	16 Up to 8,000 IPv6 prefixes for BGPv6 peering
	5720 Series	256
	7520 Series	256
	7720 Series	256

Table 27: IP Unicast Maximums (continued)

Attribute	Product	Maximum number supported
IPv6 VRFs with iBGP	4220 Series	n/a
	5320 Series	5320-16P-2MXT-2X and 48-port models: 8 5320-16P-4XE and 24-port models: 1
	5420 Series	8
	5520 Series	16
	5720 Series	16
	7520 Series	16
	7720 Series	16
BFD VRF instances	4220 Series	1
	5320 Series	48-port models: 16 5320-16P-2MXT-2X and 5320-24T-4X-XT: 8 5320-16P-4XE and other 24- port models: 1
	5420 Series	16
	5520 Series	16
	5720 Series	16
	7520 Series	16
	7720 Series	16
BFD sessions per switch (IPv4/ IPv6) with default values	4220 Series	1
	5320 Series	5320-24T-4X-XT and 48-port models: 16 16- and other 24- port models: 1
	5420 Series	16
	5520 Series	16
	5720 Series	16
	7520 Series	16
	7720 Series	16

Table 27: IP Unicast Maximums (continued)

Attribute	Product	Maximum number supported
BFD sessions per switch (IPv4) with 750ms timers for BGP and static routes only	4220 Series	1
	5320 Series	48-port models: 16 16- and 24- port models: 1
	5420 Series	16
	5520 Series	16
	5720 Series	16
	7520 Series	50
	7720 Series	50
BFD sessions with Fabric Extend tunnels (IPv4)	4220 Series	1
	5320 Series	48-port models: 16 16- and 24- port models: 1
	5420 Series	16
	5520 Series	16
	5720 Series	16
	7520 Series	16
	7720 Series	16
Virtual router IDs with Anycast IP Gateway	4220 Series	16
	5320 Series	16
	5420 Series	16
	5520 Series	16
	5720 Series	16
	7520 Series	16
	7720 Series	16

IP Interface Maximums Clarification

In the following sections, the formulas refer to "#IP Interfaces" count and not the count of IP addresses, which can be greater if you use IP multinetting with either IPv4 or IPv6. To clarify, if you use multinetting or IPv4 and IPv6 dual stack on a VLAN, the consumption of routable MAC resources is as follows:

- IPv4 address (primary) consumes one entry of routable MACs
- IPv4 address (primary) + any number of secondary addresses (multinetting) consumes one entry of routable MACs
- IPv6 interface (link-local) consumes one entry of routable MACs

- IPv6 interface (link-local) + any number of global addresses consume one entry of routable MACs
- IPv4 address (in any combination) + IPv6 interface (in any combination) consumes one entry of routable MACs

IP Interface Maximums for 4220 Series

The maximum number of IP interfaces for 4220 Series is based on the following formula:

# IP interfaces (max 128) + (# of VRRP IPv4 interfaces) + 2(if IP Shortcuts is enabled) + 3 + (#Anycast IP Gateway VLANs if Anycast IP Gateway router) = cannot exceed 128

For additional detail, see IP Interface Maximums Clarification on page 65.

IP Interface Maximums for 5320 Series

The maximum number of IP interfaces for 5320 Series is based on the following formulas:

5320-16P-2MXT-2X and 5320-24T-4X-XT

# IP interfaces (248 max) + (# of VRRP IPv4 interfaces) + (# of VRRP IPv6 interfaces) + 2(if IP Shortcuts is enabled) + 3x(# of VRFs) + (#Anycast IP Gateway VLANs if Anycast IP Gateway router) = cannot exceed 248

For additional detail, see IP Interface Maximums Clarification on page 65.

16- and Other 24-port models

# IP interfaces (max 248) + (# of VRRP IPv4 interfaces) + (# of VRRP IPv6 interfaces) + 2(if IP Shortcuts is enabled) + 3 + (#Anycast IP Gateway VLANs if Anycast IP Gateway router) = cannot exceed 248

For additional detail, see IP Interface Maximums Clarification on page 65.

48-port models

- If you disable the VRF scaling boot configuration flag:
  - # IP interfaces (248 max) + (# of VRRP IPv4 interfaces) + (# of VRRP IPv6 interfaces) + 2(if IP Shortcuts is enabled) + 3x(# of VRFs) + (#Anycast IP Gateway VLANs if Anycast IP Gateway router) = cannot exceed 248
- If you enable the VRF scaling boot configuration flag:
  - # IP interfaces (max 248) + (# of VRRP IPv4 interfaces) + (# of VRRP IPv6 interfaces) + 2(if IP Shortcuts is enabled) + 3 + (#Anycast IP Gateway VLANs if Anycast IP Gateway router) = cannot exceed 248

For additional detail, see IP Interface Maximums Clarification on page 65.

IP Interface Maximums for 5420 Series

The maximum number of IP interfaces for 5420 Series is based on the following formulas:

- If you disable the VRF scaling boot configuration flag:
    - # IP interfaces (248 max) + (# of VRRP IPv4 interfaces) + (# of VRRP IPv6 interfaces) + (# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 3x(# of VRFs) + (#Anycast Gw VLANs if Anycast Gw router) = cannot exceed 248
- If you enable the VRF scaling boot configuration flag:
    - # IP interfaces (max 248) + (# of VRRP IPv4 interfaces) + (# of VRRP IPv6 interfaces) + (# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 3 + (#Anycast Gw VLANs if Anycast Gw router) = cannot exceed 248

For additional detail, see IP Interface Maximums Clarification on page 65.

IP Interface Maximums for 5520 Series

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

- If you disable the VRF scaling boot configuration flag:
    - For interior node/non boundary node:

      #NON DVR IP Interfaces + (# of VRRP interfaces) + (# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 3x(# of VRFs) + 1(if DVR node) + (#DVR VLANs if DVR controller) + (#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000
    - For boundary node:

      #NON DVR IP Interfaces + 2x(# of VRRP interfaces) + 2x(# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 7x(# of VRFs) + 1(if DVR node) + 2x(#DVR VLANs if DVR controller) + 2x(#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000
- If you enable the VRF scaling boot configuration flag:
    - For interior node/non boundary node:

      #NON DVR IP Interfaces + (# of VRRP interfaces) + (# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 3(if L3VSN is enabled) + 1(if DVR node) + (#DVR VLANs if DVR controller) + (#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000
    - For boundary node:

      #NON DVR IP Interfaces + 2x(# of VRRP interfaces) + 2x(# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 7(if L3VSN is enabled) + 1(if DVR node) + 2x(#DVR VLANs if DVR controller) + 2x(#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000

For additional detail, see IP Interface Maximums Clarification on page 65.

IP Interface Maximums for 5720 Series

The maximum number of IP interfaces for 5720 Series is based on the following formulas:

- If you disable the VRF scaling boot configuration flag:
  - For interior node/non boundary node:

    #NON DVR IP Interfaces + (# of VRRP interfaces) + (# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 3x(# of VRFs) + 1(if DVR node) + (#DVR VLANs if DVR controller) + (#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000
  - For boundary node:

    #NON DVR IP Interfaces + 2x(# of VRRP interfaces) + 2x(# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 7x(# of VRFs) + 1(if DVR node) + 2x(#DVR VLANs if DVR controller) + 2x(#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000
- If you enable the VRF scaling boot configuration flag:
  - For interior node/non boundary node:

    #NON DVR IP Interfaces + (# of VRRP interfaces) + (# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 3(if L3VSN is enabled) + 1(if DVR node) + (#DVR VLANs if DVR controller) + (#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000
  - For boundary node:

    #NON DVR IP Interfaces + 2x(# of VRRP interfaces) + 2x(# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 7(if L3VSN is enabled) + 1(if DVR node) + 2x(#DVR VLANs if DVR controller) + 2x(#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000

For additional detail, see IP Interface Maximums Clarification on page 65.

IP Interface Maximums for 7520 Series

The maximum number of IP interfaces for 7520 Series is based on the following formulas:

- If you disable the VRF scaling boot configuration flag:
  - For interior node/non-boundary node:

    #NON DVR IP Interfaces with unique mac offset + (# of VRRP interfaces) + (# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 3x(# of VRFs) + 1(if DVR node) + (#DVR VLANs if DVR controller) + (#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000
  - For boundary node:

    #NON DVR IP Interfaces with unique mac offset + 2x(# of VRRP interfaces) + 2x(# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 7x(# of VRFs) + 1(if DVR node) + 2x(#DVR VLANs if DVR controller) + 2x(#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000

- If you enable the VRF scaling boot configuration flag:
    - For interior node/non-boundary node:

      #NON DVR IP Interfaces with unique mac offset + (# of VRRP interfaces) + (# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 3(if L3VSN is enabled) + 1(if DVR node) + (#DVR VLANs if DVR controller) + (#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000
    - For boundary node:

      #NON DVR IP Interfaces with unique mac offset + 2x(# of VRRP interfaces) + 2x(# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 7(if L3VSN is enabled) + 1(if DVR node) + 2x(#DVR VLANs if DVR controller) + 2x(#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000

For additional detail, see IP Interface Maximums Clarification on page 65.

IP Interface Maximums for 7720 Series

The maximum number of IP interfaces for 7720 Series is based on the following formulas:

- If you disable the VRF scaling boot configuration flag:
    - For interior node/non-boundary node:

      #NON DVR IP Interfaces with unique mac offset + (# of VRRP interfaces) + (# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 3x(# of VRFs) + 1(if DVR node) + (#DVR VLANs if DVR controller) + (#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000
    - For boundary node:

      #NON DVR IP Interfaces with unique mac offset + 2x(# of VRRP interfaces) + 2x(# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 7x(# of VRFs) + 1(if DVR node) + 2x(#DVR VLANs if DVR controller) + 2x(#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000
- If you enable the VRF scaling boot configuration flag:
    - For interior node/non-boundary node:

      #NON DVR IP Interfaces with unique mac offset + (# of VRRP interfaces) + (# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 3(if L3VSN is enabled) + 1(if DVR node) + (#DVR VLANs if DVR controller) + (#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000
    - For boundary node:

      #NON DVR IP Interfaces with unique mac offset + 2x(# of VRRP interfaces) + 2x(# of RSMLT interfaces) + 2(if IP Shortcuts is enabled) + 7(if L3VSN is enabled) + 1(if DVR node) + 2x(#DVR VLANs if DVR controller) + 2x(#Anycast Gw VLANs if Anycast Gw router) cannot exceed 1000

For additional detail, see IP Interface Maximums Clarification on page 65.

Layer 3 Route Table Size

Table 28: Layer 3 Route Table Size Maximums

Attribute	Maximum number supported
IPv4 RIP routes	See Route Scaling on page 70.
IPv4 OSPF routes	
IPv4 BGP routes	
IPv4 SPB shortcut routes	
IPv4 SPB Layer 3 VSN routes	
IPv6 OSPFv3 routes - GRT only	
IPv6 SPB shortcut routes - GRT only	
IPv6 RIPng routes	

Route Scaling

The following table provides information on IPv4 and IPv6 route scaling. The route table is a shared hardware resource where IPv4 routes consume one entry and IPv6 routes with a prefix length less than 64 consume two entries.

The route scaling does not depend on the protocol itself, but rather the general system limitation in the following configuration modes:

- URPF check mode - Enable this boot configuration flag to support Unicast Reverse Path Forwarding check mode.
- IPv6 mode - Enable this boot configuration flag to support IPv6 routes with prefix-lengths greater than 64 bits. When the IPv6-mode is enabled, the maximum number of IPv4 routing table entries decreases. This flag does not apply to all hardware platforms.

4220 Series

The maximum IPv4 route table size for 4220 Series is 1,000. IPv6 and URPF mode do not apply to 4220 Series.

5320 Series

Note

Only 5320-16P-2MXT-2X, 5320-24T-24S-4XE-XT , 5320-48P-8XE, and 5320-48T-8XE support URPF mode.

Model	URPF mode	IPv6 mode	IPv4	IPv6 (prefix less than 64)	IPv6 (prefix greater than 64)
48-port models	No	No	12K	6K	n/a
	No	Yes	6K	2K	1.5K
	Yes	Yes	3K	1K	750
	Yes	No	6K	2K	n/a
5320-24T-4X-XT	No	No	1K	1K	n/a
	No	Yes	500	500	250
5320-16P-4XE Other 24-port models	No	No	8K	4K	n/a
	No	Yes	4K	2K	1K
5320-16P-2MXT-2X	No	No	1,000	1,000	n/a
	No	Yes	500	500	250
	Yes	No	500	500	n/a
	Yes	Yes	250	250	125

Note:

The total number of routes include local routes.

The stated numbers in the preceding rows are one-dimensional where the given number implies that only routes for that address family or type are present. For a given row in the table, the maximum scaling number is ‘x’ IPv4 routes OR ‘y’ ipv6 <= 64 routes (not a combination of both).

5420 Series

URPF mode	IPv6 mode	IPv4	IPv6 (prefix less than 64)	IPv6 (prefix greater than 64)
No	No	12K	6K	n/a
No	Yes	6K	2K	1,500
Yes	No	6K	3K	n/a
Yes	Yes	3K	1K	750

Note:

The total number of routes include local routes.

The stated numbers in the preceding rows are one-dimensional where the given number implies that only routes for that address family or type are present. For a given row in the table, the maximum scaling number is ‘x’ IPv4 routes OR ‘y’ ipv6 <= 64 routes (not a combination of both).

5520 Series

URPF mode	IPv6 mode	IPv4	IPv6 (prefix less than 64)	IPv6 (prefix greater than 64)
No	No	16K	8K	n/a
No	Yes	8K	4K	2K
Yes	No	8K	4K	n/a
Yes	Yes	4K	2K	1K

Note:

The total number of routes include local routes.

The stated numbers in the preceding rows are one-dimensional where the given number implies that only routes for that address family or type are present. For a given row in the table, the maximum scaling number is ‘x’ IPv4 routes OR ‘y’ ipv6 <= 64 routes (not a combination of both).

5720 Series

URPF mode	IPv6 mode	IPv4	IPv6 (prefix less than 64)	IPv6 (prefix greater than 64)
No	No	5720MW Series models: 16K 5720MXW Series models: 24K	5720MW Series models: 8K 5720MXW Series models: 12K	n/a
No	Yes	5720MW Series models: 8K 5720MXW Series models: 12K	5720MW Series models: 4K 5720MXW Series models: 6K	5720MW Series models: 2K 5720MXW Series models: 3K
Yes	No	5720MW Series models: 8K 5720MXW Series models: 12K	5720MW Series models: 4K 5720MXW Series models: 6K	n/a
Yes	Yes	5720MW Series models: 4K 5720MXW Series models: 6K	5720MW Series models: 2K 5720MXW Series models: 3K	5720MW Series models: 1K 5720MXW Series models: 1.5K

Note:

The total number of routes include local routes.

The stated numbers in the preceding rows are one-dimensional where the given number implies that only routes for that address family or type are present. For a given row in the table, the maximum scaling number is 'x' IPv4 routes OR 'y' ipv6 <= 64 routes (not a combination of both).

7520 Series

URPF mode	IPv6 mode	IPv4	IPv6 (prefix less than 64)	IPv6 (prefix greater than 64)
No	No	15,000	7,000	n/a
No	Yes	7,000	3,500	2,000
Yes	No	7,000	3,500	n/a
Yes	Yes	3,000	1,500	1,000
Note: The total number of routes include local routes. The stated numbers in the preceding rows are one-dimensional where the given number implies that only routes for that address family or type are present. For a given row in the table, the maximum scaling number is 'x' IPv4 routes OR 'y' ipv6 <= 64 routes (not a combination of both).				

7720 Series

URPF mode	IPv6 mode	IPv4	IPv6 (prefix less than 64)	IPv6 (prefix greater than 64)
No	No	15,000	7,000	n/a
No	Yes	7,000	3,500	2,000
Yes	No	7,000	3,500	n/a
Yes	Yes	3,000	1,500	1,000
Note: The total number of routes include local routes. The stated numbers in the preceding rows are one-dimensional where the given number implies that only routes for that address family or type are present. For a given row in the table, the maximum scaling number is 'x' IPv4 routes OR 'y' ipv6 <= 64 routes (not a combination of both).				

IP Multicast

Table 29: IP Multicast Maximums

Attribute	Product	Maximum number supported
IGMP/MLD interfaces (IPv4/IPv6)	4220 Series	4,000/0
	5320 Series	4,000/2,000
	5420 Series	4,000/2,000
	5520 Series	4,059
	5720 Series	4,059
	7520 Series	4,059
	7720 Series	4,059

Table 29: IP Multicast Maximums (continued)

Attribute	Product	Maximum number supported
PIM interfaces (IPv4/IPv6)	4220 Series	n/a
	5320 Series	16 active
	5420 Series	16 active
	5520 Series	128 active
	5720 Series	128 active
	7520 Series	128 active
	7720 Series	128 active
PIM Neighbors (IPv4/IPv6) (GRT Only)	4220 Series	n/a
	5320 Series	16
	5420 Series	16
	5520 Series	128
	5720 Series	128
	7520 Series	128
	7720 Series	128
PIM-SSM static channels (IPv4/IPv6)	4220 Series	n/a
	5320 Series	512
	5420 Series	512
	5520 Series	4,000
	5720 Series	4,000
	7520 Series	4,000
	7720 Series	4,000
Multicast receivers/IGMP joins (IPv4/IPv6) (per switch)	4220 Series	6,000
	5320 Series	6,000
	5420 Series	6,000
	5520 Series	6,000
	5720 Series	6,000
	7520 Series	6,000
	7720 Series	6,000

Table 29: IP Multicast Maximums (continued)

Attribute	Product	Maximum number supported
Total multicast routes (S,G,V) (IPv4/IPv6) (per switch)	4220 Series	500
	5320 Series	5320-16P-2MXT-2X and 48-port models: 4,000 5320-24T-4X-XT: 500 5320-16P-4XE and other 24-port models: 2,000
	5420 Series	4,000
	5520 Series	4,000
	5720 Series	6,000
	7520 Series	6,000
	7720 Series	6,000
Total multicast routes (S,G,V) (IPv4) on an SPB-PIM Gateway configured switch	4220 Series	n/a
	5320 Series	n/a
	5420 Series	n/a
	5520 Series	4,000
	5720 Series	n/a
	7520 Series	3,000
	7720 Series	3,000
Static multicast routes (S,G,V) (IPv4/IPv6)	4220 Series	500
	5320 Series	5320-24T-4X-XT: 500 5320-16P-2MXT-2X and 48-port models: 4,000 5320-16P-4XE and other 24-port models: 2,000
	5420 Series	4,000
	5520 Series	4,000
	5720 Series	6,000
	7520 Series	4,000
	7720 Series	4,000

Table 29: IP Multicast Maximums (continued)

Attribute	Product	Maximum number supported
Multicast enabled Layer 2 VSN (IPv4)	4220 Series	64
	5320 Series	48-port models: 500 5320-24T-4X-XT: 64 5320-16P-4XE and other 24-port models: 250 5320-16P-2MXT-2X: 128
	5420 Series	500
	5520 Series	2,000
	5720 Series	2,000
	7520 Series	2,000
	7720 Series	2,000
Multicast enabled Layer 3 VSN (IPv4)	4220 Series	1
	5320 Series	48-port models: 64 5320-16P-2MXT-2X and 5320-24T-4X-XT: 8 including mgmt VRF and GRT 5320-16P-4XE and other 24-port models: 1
	5420 Series	64
	5520 Series	256 including mgmt VRF and GRT
	5720 Series	256
	7520 Series	256
	7720 Series	256
SPB-PIM Gateway controller S,Gs (source announcements) with MSDP (IPv4)	4220 Series	n/a
	5320 Series	n/a
	5420 Series	n/a
	5520 Series	6,000
	5720 Series	n/a
	7520 Series	6,000
	7720 Series	6,000

Table 29: IP Multicast Maximums (continued)

Attribute	Product	Maximum number supported
SPB-PIM Gateway controllers per SPB fabric (IPv4)	4220 Series	n/a
	5320 Series	n/a
	5420 Series	n/a
	5520 Series	5
	5720 Series	n/a
	7520 Series	5
	7720 Series	5
SPB-PIM Gateway nodes per SPB fabric (IPv4)	4220 Series	n/a
	5320 Series	n/a
	5420 Series	n/a
	5520 Series	64
	5720 Series	n/a
	7520 Series	64
	7720 Series	64
SPB-PIM Gateway interfaces per BEB (IPv4)	4220 Series	n/a
	5320 Series	n/a
	5420 Series	n/a
	5520 Series	64
	5720 Series	n/a
	7520 Series	64
	7720 Series	64
PIM neighbors per SPB-PIM Gateway node (IPv4)	4220 Series	n/a
	5320 Series	n/a
	5420 Series	n/a
	5520 Series	64
	5720 Series	n/a
	7520 Series	64
	7720 Series	64

0

Distributed Virtual Routing (DvR)

Note

Feature support differs across platforms. For more information, see *Fabric Engine and VOSS Feature Matrix*.

Local hosts use ARP entries and remote hosts use host entries. For information on IP ARP scaling, see IP Unicast on page 52.

Table 30: DvR Maximums

Attribute	Product	Maximum number supported
Note: • On the DvR leaf, you must enable the VRF scaling boot configuration flag if more than 24 VRFs are required in the DvR domain. • Scaling of a VSP 4450 Series switch controls the scaling of the DvR domain it is in. For example, if a VSP 4450 Series switch is in a DvR domain with other platforms such as VSP 4450 Series and 5420 Series, the scaling of the entire domain is limited to the scaling of the VSP 4450 Series. For VSP 4450 Series scaling information, see the VOSS Release Notes for VOSS Release 8.10.		
DvR Virtual IP interfaces	5320 Series	48-port models: 248 16- and other 24-port models: n/a
	5420 Series	247 with VIST 248 without VIST
	5520 Series	499 with vIST 500 without vIST 250 on boundary node
	5720 Series	999 with vIST 1,000 without vIST 500 on boundary node
	7520 Series	999 with vIST as interior node 1,000 without vIST as interior node 500 on boundary node
	7720 Series	999 with vIST as interior node 1,000 without vIST as interior node 500 on boundary node
DvR domains per SPB fabric	5320 Series	16
	5420 Series	16
	5520 Series	16
	5720 Series	16
	7520 Series	16
	7720 Series	16

Table 30: DvR Maximums (continued)

Attribute	Product	Maximum number supported
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.	5320 Series	n/a
	5420 Series	n/a
	5520 Series	8
	5720 Series	8
	7520 Series	8
	7720 Series	8
Leaf nodes per DvR domain	5320 Series	250
	5420 Series	250
	5520 Series	250
	5720 Series	250
	7520 Series	250
	7720 Series	250
DvR enabled Layer 2 VSNs	5320 Series	48-port models: 248 16- and other 24-port models: n/a
	5420 Series	247 with vIST 248 without vIST
	5520 Series	499 with vIST 500 without vIST 250 on boundary nodes
	5720 Series	999 with vIST 1,000 without vIST 500 on boundary nodes
	7520 Series	999 with vIST as interior node 1,000 without vIST as interior node 500 on boundary node
	7720 Series	999 with vIST as interior node 1,000 without vIST as interior node 500 on boundary node

Table 30: DvR Maximums (continued)

Attribute	Product	Maximum number supported
DvR host route scaling per DvR domain (scaling number includes local as well as foreign hosts of the Layer 2 VSN that are members of the domain) If DvR Layer 2 VSNs span DvR domains, and all DvR Controllers have an IP interface on the Layer 2 VSNs, then the DvR host scaling is network-wide, as DvR Controllers will consume as many host routes as there are hosts across all DvR domains.	5320 Series	48-port models: 16,000 16- and other 24-port models: n/a
	5420 Series	5420F Series models: 16,000 5420M Series models: 32,000
	5520 Series	48,000
	5720 Series	5720MW Series models: 64,000 5720MXW Series models: 96,000
	7520 Series	40,000
	7720 Series	40,000

VXLAN Gateway

Note
Feature support differs across platforms. For more information, see *Fabric Engine and VOSS Feature Matrix*.

Table 31: .VXLAN Gateway Maximums

Attribute	Product	Maximum number supported
MAC addresses in base interworking mode	7520 Series	80,000
	7720 Series	80,000
MAC addresses in full interworking mode	7520 Series	50,000
	7720 Series	50,000
VNI IDs per node	7520 Series	2,000
	7720 Series	2,000
VTEP destinations per node or VTEP	7520 Series	500
	7720 Series	500

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

Table 32: OVSDB protocol support for VXLAN Gateway Maximums

Attribute	Product	Maximum number supported
Maximum controllers to which a single VTEP switch can connect	7520 Series	3
	7720 Series	3

Filters, QoS, and Security

For more information, see Filter Scaling on page 85.

Table 33: Filters, QoS, and Security Maximums

Attribute	Product	Maximum number supported
Total IPv4 Ingress rules/ ACEs (Port/VLAN/InVSN based, Security/QoS filters)	4220 Series	1.024
	5320 Series	48-port models: 3,072 5320-16P-4XE and 24-port models: 1,024 5320-16P-2MXT-2X: 256
	5420 Series	Primary Bank: 2,048 Secondary Bank: 1,024
	5520 Series	Primary Bank: 1,024 Secondary Bank: 512
	5720MW Series models	Primary Bank: 3,072 Secondary Bank: 1,536
	5720MXW Series models	Primary Bank: 4,096 Secondary Bank: 2,048
	7520 Series	Primary Bank: 767 Secondary Bank: 767
	7720 Series	Primary Bank: 767 Secondary Bank: 767
Maximum number of IP Source Guard filters	4220 Series	240
	5320 Series	48-port models: 480 24-port models: 240 16-port models: 160
	5420 Series	48 access port models: 480 24 access port models: 240
	5520 Series	48 access port models: 480 24 access port models: 240
	5720 Series	48-port models: 480 24-port models: 240
	7520 Series	480
	7720 Series	240

Table 33: Filters, QoS, and Security Maximums (continued)

Attribute	Product	Maximum number supported
Total IPv4 Egress rules/ACEs (Port based, Security filters)	4220 Series	190
	5320 Series	48-port models: 400, or 144 if you enable **boot config flags ipv6-egress-filter** or **boot config flags macsec** 5320-24T-4X-XT: 190, or 62 if you enable **boot config flags ipv6-egress-filter** 5320-16P-4XE and other 24-port models: 190, or 62 if you enable **boot config flags ipv6-egress-filter** or **boot config flags macsec** 5320-16P-2MXT-2X: 248, or 120 if you enable **boot config flags ipv6-egress-filter**
	5420 Series	400 144 if you enable **boot config flags ipv6-egress-filter** or **boot config flags macsec**
	5520 Series	336 80 if you enable **boot config flags ipv6-egress-filter**
	5720 Series	5720MW Series models: 2,982, 1,446 if you enable **boot config flags ipv6-egress-filter** 5720MXW Series models: 6,000 2,982 if you enable **boot config flags ipv6-egress-filter**
	7520 Series	783 271 if you enable **boot config flags ipv6-egress-filter**
	7720 Series	783 271 if you enable **boot config flags ipv6-egress-filter**

Table 33: Filters, QoS, and Security Maximums (continued)

Attribute	Product	Maximum number supported
Total IPv6 Ingress rules/ ACEs (Port/VLAN/InVSN based, Security filters)	4220 Series	1,024
	5320 Series	5320-16P-2MXT-2X: 256 All other models: 1,024
	5420 Series	512
	5520 Series	512
	5720 Series	5720MW Series models: 1,536 5720MXW Series models: 2,048
	7520 Series	767
	7720 Series	767
Total IPv6 egress rules/ACEs (Port based, Security filters)	4220 Series	n/a
	5320 Series	48-port models: 256, 0 with MACsec 5320-24T-4X-XT: 128 16- and other 24-port models: 128, 0 with MACsec
	5420 Series	256, 0 with MACsec
	5520 Series	256
	5720 Series	5720MW Series models: 1,536 5720MXW Series models: 3,072
	7520 Series	511
	7720 Series	511
EAP (clients per port) Note: The total of EAP clients plus NEAP clients per port or per switch cannot exceed 8,192.	4220 Series	32
	5320 Series	32
	5420 Series	32
	5520 Series	32
	5720 Series	32
	7520 Series	32
	7720 Series	32

Table 34: NEAP Maximums

Product	Max # supported	Details
4220 Series	300	N/A
5320-16P-2MXT-2X 5320-24T-4X-XT	300	N/A

Table 34: NEAP Maximums (continued)

Product	Max # supported	Details
Other 5320 Series Note: The total of EAP clients plus NEAP clients per port or per switch cannot exceed 8,192. Note: Resources are shared with Switched UNI Endpoints.	800	**boot config flags macsec**: NO **boot config flags spbm-node-scaling**: NO Platform VLAN: N/A
	800 Exception: 5320-24T-24S-4XE-XT = 700	**boot config flags macsec**: YES **boot config flags spbm-node-scaling**: NO Platform VLAN: NO
	700	**boot config flags macsec**: YES **boot config flags spbm-node-scaling**: NO Platform VLAN: YES
	400	**boot config flags macsec**: N/A **boot config flags spbm-node-scaling**: YES Platform VLAN: N/A
5420 Series	800	**boot config flags macsec**: NO **boot config flags spbm-node-scaling**: NO Platform VLAN: N/A
	800	**boot config flags macsec**: YES **boot config flags spbm-node-scaling**: NO Platform VLAN: NO
	700	**boot config flags macsec**: YES **boot config flags spbm-node-scaling**: NO Platform VLAN: YES
	400	**boot config flags macsec**: N/A **boot config flags spbm-node-scaling**: YES Platform VLAN: N/A
5520 Series	4,900	N/A
5720 Series	8,192	N/A
7520 Series	8,192	N/A
7720 Series	8,192	N/A

Filter Scaling

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

4220 Series

The switch supports the following maximum limits:

- 512 non-IPv6 ingress ACLs (inPort, inVSN, or inVlan):
  - 512 ACLs with 1 ACE each that can hold either Security/QoS/both action types or
  - a combination based on the following rule: ((num ACLs + num ACEs) <= 1024)

  This maximum implies a VLAN member count of 1 for inVlan ACLs or a single I-SID for inVSN. The number of rules consumed by IPv4 inPort ACLs is not multiplied by the number of ports to which this ACL applies.
- Up to 1000 ACEs in a single ACL
- 512 IPv6 ingress ACLs (inPort):
  - 512 ACLs with 1 ACE each that can hold either Security/QoS/both action types or
  - a combination based on the following rule: (num ACLs + num ACEs) <= 1024

  This maximum also implies a port member count of 1 for the inPort ACL. The number of rules consumed by IPv6 inPort ACL is multiplied by the number of ports to which this ACL applies.
- 1024 ingress ACEs: All ACEs can hold either Security/QoS/both action types

  This maximum also implies a VLAN member count of 1 for an inVlan ACL.
- 190 egress ACEs

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

5320 Series

The 5320-16P-4XE and all 24-port models support the following maximum limits:

- 512 non-IPv6 ingress ACLs (inPort, inVSN, or inVlan):
  - 512 ACLs with 1 ACE each that can hold either Security/QoS/both action types or
  - a combination based on the following rule: ((num ACLs + num ACEs) <= 1024)

  This maximum implies a VLAN member count of 1 for inVlan ACLs or a single I-SID for inVSN. The number of rules consumed by IPv4 inPort ACLs is not multiplied by the number of ports to which this ACL applies.
- Up to 1000 ACEs in a single ACL
- 512 IPv6 ingress ACLs (inPort):
  - 512 ACLs with 1 ACE each that can hold either Security/QoS/both action types or
  - a combination based on the following rule: (num ACLs + num ACEs) <= 1024

  This maximum also implies a port member count of 1 for the inPort ACL. The number of rules consumed by IPv6 inPort ACL is multiplied by the number of ports to which this ACL applies.

- 1024 ingress ACEs: All ACEs can hold either Security/QoS/both action types

  This maximum also implies a VLAN member count of 1 for an inVlan ACL.
- 190 egress ACEs

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

The 48-port models support the following maximum limits:

> **Note**
> 5320-16P-2MXT-2X supports the same formulas but with different maximum values. See maximum values in Filters, QoS, and Security on page 81.

- 512 non-IPv6 ingress ACLs (inPort, inVSN, or inVlan):
  - 512 ACLs with 5 ACEs each that can hold either Security/QoS/both action types or
  - a combination based on the following rule: ((num ACLs + num ACEs) <= 3072)

  This maximum implies a VLAN member count of 1 for inVlan ACLs or a single I-SID for inVSN. The number of rules consumed by IPv4 inPort ACLs is not multiplied by the number of ports to which this ACL applies.
- Up to 1000 ACEs in a single ACL
- 512 IPv6 ingress ACLs (inPort):
  - 512 ACLs with 5 ACEs each that can hold either Security/QoS/both action types or
  - a combination based on the following rule: (num ACLs + num ACEs) <= 3072

  This maximum also implies a port member count of 1 for the inPort ACL. The number of rules consumed by IPv6 inPort ACL is multiplied by the number of ports to which this ACL applies.
- 1024 ingress ACEs: All ACEs can hold either Security/QoS/both action types

  This maximum also implies a VLAN member count of 1 for an inVlan ACL.
- 400 egress ACEs

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

5420 Series

The switch supports the following maximum limits:

- 512 non-IPv6 ingress ACLs (inPort, inVSN, or inVlan):
  - 512 ACLs with 3 Primary Bank ACEs each OR
  - 512 ACLs with 1 Security Bank ACE each OR
  - a combination based on the following rule:
    - ((num ACLs + num Primary Bank ACEs) <= 2048) <= ((num ACLs + num Secondary Bank ACEs) <= 1024)

This maximum implies a VLAN member count of 1 for inVlan ACLs or a single I-SID for inVSN. The number of rules consumed by IPv4 inPort ACLs is not multiplied by the number of ports to which this ACL applies.

- Up to 1000 ACEs in a single ACL
- 512 IPv6 ingress ACLs (inPort):
    - 512 ACLs with 1 ACE each OR
    - a combination based on the following rule:
        - (num ACLs + num IPv6 ACEs + num IPv4 Secondary Bank ACEs) <= 1024

  This maximum also implies a port member count of 1 for the inPort ACL. The number of rules consumed by IPv6 inPort ACLs is multiplied by the number of ports to which this ACL applies.
- 3072 ingress ACEs:

  Theoretical maximum of 1024 implies 1 ingress ACL with 512 Primary Bank ACEs and 512 Secondary Bank ACEs
    - Ingress ACEs supported: (2048 (Primary Bank) - # of ACLs) + (1024 (Secondary Bank) - # of ACLs)

  This maximum also implies a VLAN member count of 1 for an inVlan ACL.
- 400 egress ACEs:

  Theoretical maximum of 400 implies 1 egress ACL with 400 ACEs
    - Egress ACEs supported: 400 - # of ACLs .

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

5520 Series

The switch supports the following maximum limits:

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

  This maximum implies a VLAN member count of 1 for inVlan ACLs or a single I-SID for inVSN. The number of rules consumed by IPv4 inPort ACLs is not multiplied by the number of ports to which this ACL applies.
- Up to 1000 ACEs in a single ACL
- 512 IPv6 ingress ACLs (inPort):
    - 512 ACLs with 1 ACE each OR
    - a combination based on the following rule:
        - (num ACLs + num ACEs + num IPv4 Security Bank ACEs) <= 512

The number of rules consumed by IPv6 ingress ACLs inPort ACLs is multiplied by the number of ports to which this ACL applies.

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

  This maximum implies a port member count of 1 for outPort ACLs.
- 1536 ingress ACEs:
  - Ingress ACEs supported: (1024 (Primary Bank) - # of ACLs) + (512 (Secondary Bank) - # of ACLs)
- 247 egress ACEs:
  - Egress ACEs supported: 248 - # of ACLs

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

5720-24MW and 5720-48MW

The switch supports the following maximum limits:

- 512 non-IPv6 ingress ACLs (inPort, inVSN, or inVlan):
  - 512 ACLs with 5 Primary Bank ACEs each OR
  - 512 ACLs with 2 Secondary Bank ACEs each OR
  - a combination based on the following rule:
    - ((num ACLs + num Primary Bank ACEs) <= 3072) && ((num ACLs + num Security Bank ACEs) <= 1536)

  This maximum implies a VLAN member count of 1 for inVlan ACLs or a single I-SID for inVSN.

  The number of rules consumed by IPv4 inPort ACLs is not multiplied by the number of ports to which this ACL applies.
- You can configure up to 1000 ACEs in a single ACL.
- 512 IPv6 ingress ACLs (inPort):
  - 512 ACLs with 2 ACEs each OR
  - a combination based on the following rule:
    - (num ACLs + num ACEs + num of IPv4 Security Bank ACEs) <= 1536

  The number of rules consumed by IPv6 inPort ACLs is multiplied by the number of ports to which this ACL applies.
- 256 egress ACLs (outPort only):
  - 1 OR
  - a combination based on the following rule:
    - (num ACLs + num ACES) <=2982
- 4608 ingress ACEs

Ingress ACEs supported: (3072 Primary Bank - num ACLs) + (1536 Secondary Bank - num ACEs)

- 2982 egress ACEs

  Egress ACEs supported: 2982 - num ACLs

5720-24MXW and 5720-48MXW

The switch supports the following maximum limits:

- 512 non-IPv6 ingress ACLs (inPort, inVSN, or inVlan):
  - 512 ACLs with 7 Primary Bank ACEs each OR
  - 512 ACLs with 3 Secondary Bank ACEs each OR
  - a combination based on the following rule:
    - ((num ACLs + num Primary Bank ACEs) <= 4096) && ((num ACLs + num Security Bank ACEs) <= 2048)

  This maximum implies a VLAN member count of 1 for inVlan ACLs or a single I-SID for inVSN.

  The number of rules consumed by IPv4 inPort ACLs is not multiplied by the number of ports to which this ACL applies.
- You can configure up to 1000 ACEs in a single ACL.
- 512 IPv6 ingress ACLs (inPort):
  - 512 ACLs with 3 ACEs each OR
  - a combination based on the following rule:
    - (num ACLs + num ACEs + num of IPv4 Security Bank ACEs) <= 2048

  The number of rules consumed by IPv6 inPort ACLs is multiplied by the number of ports to which this ACL applies.
- 256 egress ACLs (outPort only):
  - 1 OR
  - a combination based on the following rule:
    - (num ACLs + num ACES) <=6000
- 6144 ingress ACEs

  Ingress ACEs supported: (4096 Primary Bank - num ACLs) + (2048 Secondary Bank - num ACEs)
- 6000 egress ACEs

  Egress ACEs supported: 6000 - num ACLs

7520 Series

The switch supports the following maximum limits for ACL scaling:

- 512 non-IPv6 ingress ACLs (inVSN, inPort, or inVlan):
  - 256 ACLs with 1 Primary ACE each + 256 ACLs with 1 Secondary ACE each OR
  - 383 ACLs with 1 Primary ACE each and/or 1 Secondary ACE each OR

    - a combination based on the following rule:
        - num ACLs <= 512 && (num ACLs + num Primary ACEs) <= 767 && (num ACLs + num Secondary ACEs) <= (767 – X) where X = num IPv6 ACLs + num IPv6 ACEs

  For Primary bank, maximum implies a single port on inPort ACLs, a single I-SID for in VSN, and a single VLAN on inVlan ACLs.

  For Secondary bank, inPort ACLs number of consumed rules is not multiplied by the number of ports attached to the ACL.

- 383 IPv6 ingress ACLs (inPort):
    - 383 IPv6 ACLs with 1 ACE each OR
    - A combination based on the following rule:
        - num IPv6 ACLs <= 383 && (num IPv6 ACLs + num ACEs) <= (767 – X) where X = num non-IPv6 ACLs + num non-IPv6 Secondary ACEs

  This maximum implies a single port on inPort ACLs.

- 254 non-IPv6 egress ACLs (outPort):
    - 254 ACLS with 1 Security ACE each OR
        - A combination based on the following rule:
            - num ACLs <= 254 && (num ACLs + num Security ACEs) <= 508

  This maximum implies a single port on outPort ACLs.

- 256 IPv6 Egress ACLs (outPort):
    - 256 ACLS with 1 Security ACE each OR
    - A combination based on the following rule:
        - num ACLs <= 256 && (num ACLs + num Security ACEs) <= 512

  This maximum implies a single port on outPort ACLs.

The switch supports the following maximum limits for ACE scaling:

- 1,532 non-IPv6 ingress ACEs

  This theoretical maximum implies
    - 2 non-IPv6 ingress ACL with 383+384 Primary ACEs and 383+384 Secondary ACEs
    - no IPv6 ACLs configured
    - a single port on inPort ACLs, and a single VLAN on inVLAN ACLs
- 767 IPv6 ingress ACEs

  This theoretical maximum implies
    - 1 IPv6 ingress ACL with 767 Security ACEs
    - no non-IPv6 ACLs configured
    - a port member count of 1 for inPort ACLs
- 783 non-IPv6 egress ACEs.

  This theoretical maximum implies

  - 1 egress ACL with 783 Security ACEs
  - a port member count of 1 for outPort ACLs
  - Non IPv6 egress ACEs supported: 783 - num non-IPv6 egress ACLs

- 511 IPv6 egress ACEs

  This theoretical maximum implies

  - 1 egress ACL with 511 Security ACEs
  - a port member count of 1 for outPort ACLs
  - 511 - num IPv6 egress ACLs

7720 Series

The switch supports the following maximum limits for ACL scaling:

- 512 non-IPv6 ingress ACLs (inVSN, inPort, or inVlan):
  - 256 ACLs with 1 Primary ACE each + 256 ACLs with 1 Secondary ACE each OR
  - 383 ACLs with 1 Primary ACE each and/or 1 Secondary ACE each OR
  - a combination based on the following rule:
    - num ACLs <= 512 && (num ACLs + num Primary ACEs) <= 767 && (num ACLs + num Secondary ACEs) <= (767 – X) where X = num IPv6 ACLs + num IPv6 ACEs

  For Primary bank, maximum implies a single port on inPort ACLs, a single I-SID for in VSN, and a single VLAN on inVlan ACLs.

  For Secondary bank, inPort ACLs number of consumed rules is not multiplied by the number of ports attached to the ACL.
- 383 IPv6 ingress ACLs (inPort):
  - 383 IPv6 ACLs with 1 ACE each OR
  - A combination based on the following rule:
    - num IPv6 ACLs <= 383 && (num IPv6 ACLs + num ACEs) <= (767 – X) where X = num non-IPv6 ACLs + num non-IPv6 Secondary ACEs

  This maximum implies a single port on inPort ACLs.
- 254 non-IPv6 egress ACLs (outPort):
  - 254 ACLS with 1 Security ACE each OR
    - A combination based on the following rule:
      - num ACLs <= 254 && (num ACLs + num Security ACEs) <= 508

  This maximum implies a single port on outPort ACLs.
- 256 IPv6 Egress ACLs (outPort):
  - 256 ACLS with 1 Security ACE each OR
  - A combination based on the following rule:
    - num ACLs <= 256 && (num ACLs + num Security ACEs) <= 512

  This maximum implies a single port on outPort ACLs.

The switch supports the following maximum limits for ACE scaling:

- 1,532 non-IPv6 ingress ACEs

  This theoretical maximum implies

  - 2 non-IPv6 ingress ACL with 383+384 Primary ACEs and 383+384 Secondary ACEs
  - no IPv6 ACLs configured
  - a single port on inPort ACLs, and a single VLAN on inVLAN ACLs
- 767 IPv6 ingress ACEs

  This theoretical maximum implies

  - 1 IPv6 ingress ACL with 767 Security ACEs
  - no non-IPv6 ACLs configured
  - a port member count of 1 for inPort ACLs
- 783 non-IPv6 egress ACEs.

  This theoretical maximum implies

  - 1 egress ACL with 783 Security ACEs
  - a port member count of 1 for outPort ACLs
  - Non IPv6 egress ACEs supported: 783 - num non-IPv6 egress ACLs
- 511 IPv6 egress ACEs

  This theoretical maximum implies

  - 1 egress ACL with 511 Security ACEs
  - a port member count of 1 for outPort ACLs
  - 511 - num IPv6 egress ACLs

Routed Private VLANs/E-TREEs Scaling

The number of private VLANs that you configure with an IP address influences the IPv4 Egress ACE count.

The following table lists scaling limits for Routed Private VLANs/E-TREEs. Limits are not enforced; either number of private VLANs or number of private VLAN trunk ports can go beyond the recommended values.

Table 35: Routed Private VLANs/E-TREEs Maximums

	Private VLAN trunk ports	Routed PVLANs/E-TREEs	IPv4 Egress ACE rules available (No IPv6 egress filter bootflag enabled)	IPv4 Egress ACE rules available (With IPv6 egress filter bootflag enabled)
5320-24T-24S-4XE-XT 5320-48T-8XE 5320-48P-8XE	4	10	349	93
5320-16P-4XE 5320-16P-4XE-DC 5320-16P-2MXT-2X 5320-24P-8XE 5320-24T-8XE	4	10	139	11
5420 Series	4	10	349	93
5520 Series	4	10	285	29
5720-24MW 5720-48MW	4	100	2499	999
5720-24MXW 5720-48MXW	4	100	5499	2499
7520 Series	4	50	783	271
7720 Series	4	50	783	271

Use the **`show io resources filter`** command to verify remaining resources. This command displays the following information:

- resources consumed by Routed Private VLANs
- free entries available for either IPv4 Egress ACEs or private VLANs

The following example output displays resource usage on a 5320 Series switch with one Routed Private VLAN and one outPort ACL.

```
Switch:1>show io resources filter
=============================================================================
                                  FILTER TABLE
=============================================================================
-----------------------------------------------------------------------------
ACL Filter Resource Manager stats
----------------------------------------------------------------------------
BCM CAP Group: |  ICAP_SEC_QOS | ICAP_IPv6 | ECAP_SEC  | ECAP_IPv6
    Group Mode: | Double        | Double    | Double    | Double
----------------------------------------------------------------------------
Total Entries: |      1024     |    1024   |     247   |     128
  Free Entries: |      1024     |    1024   |     243   |     128
```

```
        In Use: |         0      |        0   |        4   |        0
Filter table:
-----------------------------------------------------------------
  ACL |        |Port/Vlan|  Sec   |  QoS   |  All   |
  ID  | Flags  | Members | ACE's | ACE's | ACE's | Type
-----------------------------------------------------------------
    1 |00002008|      1  |    0  |    0  |    1  | outPort, non-IPv6
-----------------------------------------------------------------

Filter resources used by other features:
-------------------------------------
Feature | Type | Number of entries |
-------------------------------------
  PVlan  | ECAP |          2        |
-------------------------------------
```

OAM and Diagnostics

Table 36: OAM and Diagnostics Maximums

Attribute	Product	Maximum number supported
EDM sessions	4220 Series	5
	5320 Series	5
	5420 Series	5
	5520 Series	5
	5720 Series	5
	7520 Series	5
	7720 Series	5
FTP sessions (IPv4/IPv6)	4220 Series	8 total (4 for IPv4 and 4 for IPv6)
	5320 Series	8 total (4 for IPv4 and 4 for IPv6)
	5420 Series	8 total (4 for IPv4 and 4 for IPv6)
	5520 Series	8 total (4 for IPv4 and 4 for IPv6)
	5720 Series	8 total (4 for IPv4 and 4 for IPv6)
	7520 Series	8 total (4 for IPv4 and 4 for IPv6)
	7720 Series	8 total (4 for IPv4 and 4 for IPv6)

Table 36: OAM and Diagnostics Maximums (continued)

Attribute	Product	Maximum number supported
SSH sessions (IPv4/IPv6)	4220 Series	8 total (any combination of IPv4 and IPv6)
	5320 Series	8 total (any combination of IPv4 and IPv6)
	5420 Series	8 total (any combination of IPv4 and IPv6)
	5520 Series	8 total (any combination of IPv4 and IPv6)
	5720 Series	8 total (any combination of IPv4 and IPv6)
	7520 Series	8 total (any combination of IPv4 and IPv6)
	7720 Series	8 total (any combination of IPv4 and IPv6)
Telnet sessions (IPv4/IPv6)	4220 Series	16 total (8 for IPv4 and 8 for IPv6)
	5320 Series	16 total (8 for IPv4 and 8 for IPv6)
	5420 Series	16 total (8 for IPv4 and 8 for IPv6)
	5520 Series	16 total (8 for IPv4 and 8 for IPv6)
	5720 Series	16 total (8 for IPv4 and 8 for IPv6)
	7520 Series	16 total (8 for IPv4 and 8 for IPv6)
	7720 Series	16 total (8 for IPv4 and 8 for IPv6)
TFTP sessions (IPv4/IPv6)	4220 Series	2 total (any combination of IPv4 and IPv6)
	5320 Series	2 total (any combination of IPv4 and IPv6)
	5420 Series	2 total (any combination of IPv4 and IPv6)
	5520 Series	2 total (any combination of IPv4 and IPv6)
	5720 Series	2 total (any combination of IPv4 and IPv6)
	7520 Series	2 total (any combination of IPv4 and IPv6)
	7720 Series	2 total (any combination of IPv4 and IPv6)

Table 36: OAM and Diagnostics Maximums (continued)

Attribute	Product	Maximum number supported
Mirrored ports (source)	4220 Series	28
	5320 Series	48-port models: 56 5320-24T-4X-XT: 28 Other 24-port models: 32 5320-16P-2MXT-2X: 16 5320-16P-4XE: 20
	5420 Series	56
	5520 Series	48-port models: 47 (up to 58 with channelization) 24-port models: 23 (up to 34 with channelization)
	5720 Series	64
	7520 Series	32 (up to 125 with channelization)
	7720 Series	32 (up to 125 with channelization)
Mirroring ports (destination)	4220 Series	4
	5320 Series	4
	5420 Series	4
	5520 Series	4
	5720 Series	4
	7520 Series	4
	7720 Series	4

Table 36: OAM and Diagnostics Maximums (continued)

Attribute	Product	Maximum number supported
Fabric RSPAN Port mirror instances per switch (Ingress only)	4220 Series	Port mirror sessions can be mapped to 24 unique I-SID offsets for Ingress Mirror. Only one I-SID offset for Egress Mirror.
	5320 Series	5320-16P-2MXT-2X: Port mirror sessions can be mapped to 8 unique I-SID offsets for Ingress Mirror. Only one I-SID offset for Egress Mirror. Other models: Port mirror sessions can be mapped to 24 unique I-SID offsets for Ingress Mirror. Only one I-SID offset for Egress Mirror.
	5420 Series	Port mirror sessions can be mapped to 24 unique I-SID offsets for Ingress Mirror. Only one I-SID offset for Egress Mirror.
	5520 Series	Port mirror sessions can be mapped to 24 unique I-SID offsets for Ingress Mirror. Only one I-SID offset for Egress Mirror.
	5720 Series	Port mirror sessions can be mapped to 24 unique I-SID offsets for Ingress Mirror. Only one I-SID offset for Egress Mirror.
	7520 Series	Port mirror sessions can be mapped to 24 unique I-SID offsets for Ingress Mirror. Only one I-SID offset for Egress Mirror.
	7720 Series	Port mirror sessions can be mapped to 24 unique I-SID offsets for Ingress Mirror. Only one I-SID offset for Egress Mirror.

Table 36: OAM and Diagnostics Maximums (continued)

Attribute	Product	Maximum number supported
Fabric RSPAN Flow mirror instances per switch (Ingress only)	4220 Series	Filter ACL ACE sessions can be mapped to 24 unique I-SID offsets.
	5320 Series	5320-16P-2MXT-2X: Filter ACL ACE sessions can be mapped to 8 unique I-SID offsets. Other models: Filter ACL ACE sessions can be mapped to 24 unique I-SID offsets.
	5420 Series	Filter ACL ACE sessions can be mapped to 24 unique I-SID offsets.
	5520 Series	Filter ACL ACE sessions can be mapped to 24 unique I-SID offsets.
	5720 Series	Filter ACL ACE sessions can be mapped to 24 unique I-SID offsets.
	7520 Series	Filter ACL ACE sessions can be mapped to 24 unique I-SID offsets.
	7720 Series	Filter ACL ACE sessions can be mapped to 24 unique I-SID offsets.
Fabric RSPAN Monitoring I-SIDs (network value) Monitoring I-SIDs across SPB network	4220 Series	50
	5320 Series	48-port models: 500 5320-24T-4X-XT: 50 5320-16P-4XE and other 24-port models: 250 5320-16P-2MXT-2X: 8
	5420 Series	500
	5520 Series	1,000
	5720 Series	1,000
	7520 Series	1,000
	7720 Series	1,000

Table 36: OAM and Diagnostics Maximums (continued)

Attribute	Product	Maximum number supported
sFlow sampling limit (samples per second)	4220 Series	3,100
	5320 Series	3,100
	5420 Series	3,100 s
	5520 Series	3,100
	5720 Series	3,100
	7520 Series	3,100
	7720 Series	3,100
IPFIX flows	4220 Series	n/a
	5320 Series	48-port models: 9,000 16- and 24-port models: n/a
	5420 Series	9,000
	5520 Series	36,863
	5720 Series	5720MW models: 32,000 5720MXW models: 256,000
	7520 Series	32,767
	7720 Series	32,767
Application Telemetry host monitoring - maximum number of monitored hosts Note: These resources are shared with the IPv4 Filter Ingress rules/ ACEs.	4220 Series	382 hosts
	5320 Series	382 hosts
	5420 Series	382 hosts
	5520 Series	382 hosts
	5720 Series	382 hosts
	7520 Series	382 hosts
	7720 Series	382 hosts

Extreme Integrated Application Hosting Scaling

Note

The scaling attributes in this section apply to the following switches:

- 5720 Series models:
  - 5720-24MXW
  - 5720-48MXW
- 7520 Series
- 7720 Series

Table 37: Extreme Integrated Application Hosting (IAH) Maximums

Attribute	Product	Maximum number supported
Simultaneous Virtual Machines	5720-24MXW	2
	5720-48MXW	2
	7520 Series	6
	7720 Series	6
CPU cores available to VMs	5720-24MXW	2
	5720-48MXW	2
	7520 Series	6
	7720 Series	6
Memory available to VMs	5720-24MXW	4 GB
	5720-48MXW	4 GB
	7520 Series	12 GB
	7720 Series	12 GB
Storage available to VMs	5720-24MXW	104 GB of 120 modular SSD
	5720-48MXW	104 GB of 120 modular SSD
	7520 Series	100 GB
	7720 Series	100 GB
Total SRIOV vports available to VMs	5720-24MXW	16
	5720-48MXW	16
	7520 Series	16
	7720 Series	16
Vports available to single VM	5720-24MXW	16
	5720-48MXW	16
	7520 Series	16
	7720 Series	16

Fabric Scaling

This section lists the fabric scaling information.

Table 38: Fabric maximums

Attribute	Product	Maximum number supported (with and without vIST)
Number of SPB IS-IS areas	4220 Series	1
	5320 Series	1
	5420 Series	1
	5520 Series as boundary node	2
	5720 Series as boundary node	2
	7520 Series as boundary node	2
	7720 Series as boundary node	2
Number of B-VIDs	4220 Series	2
	5320 Series	2
	5420 Series	2
	5520 Series	2
	5720 Series	2
	7520 Series	2
	7720 Series	2
Maximum number of Physical and Logical (Fabric Extend) NNI interfaces/adjacencies (Home and Remote area total when operating as Boundary Node)	4220 Series (cannot operate as boundary node)	12
	5320 Series (cannot operate as boundary node)	5320-16P-2MXT-2X and 5320-24T-4X-XT: 12 All other models: 64
	5420 Series (cannot operate as boundary node)	50
	5520 Series	128
	5720 Series	128, of which 64 can be with IPsec using Fabric IPsec Gateway
	7520 Series	255, of which 64 can be with IPsec using Fabric IPsec Gateway
	7720 Series	255, of which 64 can be with IPsec using Fabric IPsec Gateway

Table 38: Fabric maximums (continued)

Attribute	Product	Maximum number supported (with and without vIST)
I-SIDs supported (local UNI present on device)	4220 Series	See Number of I-SIDs supported
	5320 Series	See Number of I-SIDs supported
	5420 Series	See Number of I-SIDs supported
	5520 Series	See Number of I-SIDs supported
	5720 Series	See Number of I-SIDs supported
	7520 Series	See Number of I-SIDs supported
	7720 Series	See Number of I-SIDs supported
Maximum number of Layer 2 VSNs per switch (local UNI present on device)	4220 Series	64
	5320 Series	48-port models: 500 5320-24T-4X-XT: 64 5320-16P-4XE and other 24-port models: 250 5320-16P-2MXT-2X: 128
	5420 Series	500
	5520 Series	3,580
	5720 Series	4,000
	7520 Series	4,000
	7720 Series	4,000
Maximum number of Transparent Port UNIs per switch	4220 Series	28
	5320 Series	48-port models: 52 24-port models: 28 5320-16P-4XE: 20 5320-16P-2MXT-2X: 16
	5420 Series	56
	5520 Series	48-port models: 48 24-port models: 24
	5720 Series	60
	7520 Series	56 (up to 125 with channelization)
	7720 Series	32 (up to 125 with channelization)

Table 38: Fabric maximums (continued)

Attribute	Product	Maximum number supported (with and without vIST)
Maximum number of Layer 2 E-Tree/PVLAN UNIs per switch	4220 Series	5
	5320 Series	48-port models: 50 16-port and other 24-port models: 20
	5420 Series	100
	5520 Series	200
	5720 Series	100
	7520 Series	100
	7720 Series	100
Maximum number of routed PVLANs/E-Trees	4220 Series	n/a
	5320 Series	10
	5420 Series	10
	5520 Series	10
	5720 Series	100
	7520 Series	50
	7720 Series	50
Maximum number of Layer 3 VSNs per switch See VRF Scaling on page 111.	4220 Series	1
	5320 Series	48-port models: 64 5320-16P-2MXT-2X and 5320-24T-4X-XT: 8, including mgmt VRF and GRT 5320-16P-4XE and other 24-port models: 1 local VRF and 23 remote accepted I-SIDs
	5420 Series	64
	5520 Series	256 including mgmt VRF and GRT
	5720 Series	256
	7520 Series	256
	7720 Series	256

Table 38: Fabric maximums (continued)

Attribute	Product	Maximum number supported (with and without vIST)
Maximum number of FA I-SID/ VLAN assignments per port	4220 Series	64
	5320 Series	5320-16P-2MXT-2X: 128 5320-24T-4X-XT: 64 All other models: 94
	5420 Series	94
	5520 Series	94
	5720 Series	94
	7520 Series	94
	7720 Series	94
Maximum number of IP multicast S,Gs when operating as a BCB (intra-area)	4220 Series	16,000
	5320 Series	16,000
	5420 Series	16,000
	5520 Series	16,000
	5720 Series	50,000
	7520 Series	50,000
	7720 Series	50,000
ISW switches in a Fabric Attach Ring		128
Maximum number of SD-WAN tunnels signaled on an Auto-sense port	4220 Series	115
	5320 Series	115
	5420 Series	115
	5520 Series	115
	5720 Series	115
	7520 Series	125
	7720 Series	125

Table 39: Multidimensional Fabric node scale

Device	Node scaling[1]	SPBM nodes[2]	Total unicast BMACs[3]	Switched UNI endpoints [4]	Multicast Data I-SIDs[5]	
					Ingress BEB	Egress BEB
4220 Series	n/a	128	128	300	64	64
5320-16P-2MXT-2X	n/a	300	300	300	128	128
5320-24T-4X-XT	n/a	128	128	300	64	64

Table 39: Multidimensional Fabric node scale (continued)

Device	Node scaling[1]	SPBM nodes[2]	Total unicast BMACs[3]	Switched UNI endpoints [4]	Multicast Data I-SIDs[5]	
					Ingress BEB	Egress BEB
Other 5320 Series	Enabled	500	500	400	16- and 24-port models: 250 48-port models: 500	1,200
	Disabled	350	350	700/800	16- and 24-port models: 250 48-port models: 500	800
5420 Series	Enabled	500 without vIST 340 with vIST	500 without vIST 340 with vIST	400	500	1,200
	Disabled	350 without vIST 340 with vIST	350 without vIST 340 with vIST	700/800	500	800
5520 Series		500/800	800	2,700	2,700	4,000
5720 Series		500/1,000	2,000	4,850	4,000	6,000
7520 Series		500/1,000	2,000	12,000	4,000	6,000
7720 Series		500/1,000	2,000	12,000	4,000	6,000

1. Node scaling—refers to the enabled state of the **`boot configuration flags spbm-node-scaling`** command, if applicable. For 5320 Series and 5420 Series using Fabric Extend or vIST, it is a best practice to enable this command.
2. SPBM nodes—refers to the number of supported SPBM enabled nodes, both BEB and BCB. When different, the number is formatted as per area/total per device. For 5420 Series, this number is impacted by vIST.
3. Total unicast BMACs—refers to the total number, both virtual and physical, this node can share services with. This number includes Layer 2 VSNs, Layer 3 VSNs, E-TREE, Multicast, and Transparent Port UNI. For 5420 Series, this number is impacted by vIST.
4. Switched UNI endpoints—refers to the maximum local tagged and untagged endpoints, either manual, RADIUS, or FA-assigned. When different, the number is formatted based on the configuration of the **`boot config flags macsec`** command: enabled/disabled.
5. Multicast Data I-SIDs—refers to the maximum Layer 2 or Layer 3, dynamic and static originated data I-SIDs. The overall limits are across all locally configured Layer 2 VSNs

The following table provides numbers for 5320 Series and 5420 Series only, to reflect the impact of the **`boot configuration flags spbm-node-scaling`** command, if supported.

Table 40: Maximum remote multicast sender nodes and local I-SIDs

Device	Node scaling[1]	Total remote multicast sender nodes[2]	Total local I-SIDs[3]
4220 Series	n/a	64	64
5320-24T-4X-XT	n/a	64	64
5320-16P-2MXT -2X	n/a	128	128
Other 5320 Series	Enabled	200	16- and 24-port models: 274 48-port models: 500
	Disabled	150	16- and 24-port models: 274 48-port models: 564
5420 Series	Enabled	200	500
	Disabled	150	564

1. Node scaling—refers to the enabled state of the **`boot configuration flags spbm-node-scaling`** command. For 5320 Series and 5420 Series using Fabric Extend or vIST, it is a best practice to enable this command.
2. Total remote multicast sender nodes—refers to the total number of nodes that send IP multicast streams that the local BEB receives. This space is shared with unicast BMACs in the preceding table. Documented limits are individual in isolation; introducing vIST clusters or nodes that advertise IP multicast streams decreases the total number of physical nodes in an area.
3. Total local I-SIDs— refers to the total for Layer 2, Layer 3, and Multicast. On 48-port switches, which includes 5320-24T-24S-4XE-XT, with node-scaling enabled, a number of Layer 2 VSN entries equal to the number of ports is reserved for Switched UNI untagged endpoints.

Multi-area SPB Maximums

Table 41: Multi-area SPB Maximums

Scaling	5520 Series	5720 Series	7520 Series	7720 Series
Number of nodes that can function as Multi-area SPB boundary nodes between two areas	2	2	4 in a non-vIST configuration, 2 in a vIST configuration	4 in a non-vIST configuration, 2 in a vIST configuration
SPBM enabled nodes per area	500	500	500	500
SPBM total nodes home + remote	650	650	1,000	1,000

Table 41: Multi-area SPB Maximums (continued)

Scaling	5520 Series	5720 Series	7520 Series	7720 Series
I-SIDs supported on boundary nodes (no local UNI present on device)	2,000	2,000	9,600	9,600
Maximum number of inter-area redistributed Layer 2 VSNs (no local UNI present on Boundary Node)	2,000	2,000	9,600	9,600
Maximum number of IP multicast S,Gs when operating as a boundary node (inter-area)	1,600	1,600	4,800	4,800
DvR host routes redistributed across area boundary	n/a	6,000	13,900	13,900
SPBM multicast-FIB entries	10,000	20,000	35,000	35,000

Number of I-SIDs Supported for the Number of Configured IS-IS Interfaces and Adjacencies

The number of I-SIDs supported depends on the number of IS-IS interfaces and adjacencies (NNIs) configured.

The following table shows the number of UNI I-SIDs supported per BEB. UNI I-SIDs are used for Layer 2 VSN, Layer 3 VSN, Transparent-UNI, E-Tree, Switched-UNI and S, G for Multicast.

Number of IS-IS interfaces (NNIs)	Product	I-SIDs with vIST configured on the platform	I-SIDs without vIST configured on the platform
4	4220 Series	n/a	64
	5320 Series	n/a	500 5320-16P-2MXT-2X supports a maximum of 128 5320-24T-4X-XT supports a maximum of 64
	5420 Series	564	564
	5520 Series	4,000	4,000
	5720 Series	4,000	4,000
	7520 Series	4,000	4,000
	7720 Series	4,000	4,000
6	4220 Series	n/a	64
	5320 Series	n/a	500 5320-16P-2MXT-2X supports a maximum of 128 5320-24T-4X-XT supports a maximum of 64
	5420 Series	564	564
	5520 Series	3,500	4,000
	5720 Series	3,500	4,000
	7520 Series	4,000	4,000
	7720 Series	4,000	4,000
10	4220 Series	n/a	64
	5320 Series	n/a	500 5320-16P-2MXT-2X supports a maximum of 128 5320-24T-4X-XT supports a maximum of 64
	5420 Series	564	564
	5520 Series	2,900	4,000
	5720 Series	2,900	4,000
	7520 Series	2,900	4,000
	7720 Series	2,900	4,000

Number of IS-IS interfaces (NNIs)	Product	I-SIDs with vIST configured on the platform	I-SIDs without vIST configured on the platform
20	4220 Series	n/a	n/a
	5320 Series	n/a	500 5320-16P-2MXT-2X: n/a 5320-24T-4X-XT: n/a
	5420 Series	564	564
	5520 Series	2,000	4,000
	5720 Series	2,000	4,000
	7520 Series	2,000	4,000
	7720 Series	2,000	4,000
48	4220 Series	n/a	n/a
	5320 Series	n/a	500 5320-16P-2MXT-2X : n/a 5320-24T-4X-XT: n/a
	5420 Series	564	564
	5520 Series	1,000	2,000
	5720 Series	1,000	2,000
	7520 Series	1,000	2,000
	7720 Series	1,000	2,000
72	4220 Series	n/a	n/a
	5320 Series	n/a	n/a
	5420 Series	n/a	n/a
	5520 Series	750	1,500
	5720 Series	750	1,500
	7520 Series	750	1,500
	7720 Series	750	1,500
100	4220 Series	n/a	n/a
	5320 Series	n/a	n/a
	5420 Series	n/a	n/a
	5520 Series	550	1,100
	5720 Series	550	1,100
	7520 Series	550	1,100
	7720 Series	550	1,100

Number of IS-IS interfaces (NNIs)	Product	I-SIDs with vIST configured on the platform	I-SIDs without vIST configured on the platform
128	4220 Series	n/a	n/a
	5320 Series	n/a	n/a
	5420 Series	n/a	n/a
	5520 Series	450	900
	5720 Series	450	900
	7520 Series	450	900
	7720 Series	450	900
250	4220 Series	n/a	n/a
	5320 Series	n/a	n/a
	5420 Series	n/a	n/a
	5520 Series	n/a	n/a
	5720 Series	n/a	n/a
	7520 Series	n/a	n/a
	7720 Series	n/a	n/a

Interoperability Considerations for IS-IS External Metric

BEBs running VOSS 5.0 can advertise routes into IS-IS with the metric type as external. They can also correctly interpret route advertisements with metric type external received by means of IS-IS. In an SPB network with a mix of products running different versions of software releases, you must take care to ensure that turning on the ability to use metric-type external does not cause unintended loss of connectivity.

Note the following before turning on IS-IS external metric if the SPB network has switches running a release prior to VOSS 5.0:

- There are no special release or product type implications if the switch does not have IP Shortcuts or Layer 3 VSN enabled. For example, this applies to Layer 2 only BEBs and BCBs.
- There are no special release or product type implications if the Layer 3 VSN in which routes are being advertised with a metric-type of external is not configured on the switch.
- If a switch running a VOSS release that is prior to VOSS 5.0 but VOSS 4.2.1 or later, it will treat all IS-IS routes as having metric-type internal, regardless of the metric-type (internal or external) used by the advertising BEB in its route advertisement.
- Switches running VSP 9000 Series release 4.1.0.0 or later will treat all IS-IS routes as having metric-type internal, regardless of the metric-type (internal or external) used by the advertising BEB in its route advertisement.
- Switches running VOSS releases prior to 4.2.1.0 might not correctly install IS-IS routes in a Layer 3 VSN if any routes advertised with metric-type external are advertised in that Layer 3 VSN by other BEBs in the network. Layer 3 VSNs in which there are no

routes with an external metric-type will not be impacted. Similar note applies to the GRT.

- Switches running VSP 9000 Series releases prior to 4.1.0.0 might not correctly install IS-IS routes in a Layer 3 VSN if any routes advertised with metric-type external are advertised in that Layer 3 VSN by other BEBs in the network. Layer 3 VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to GRT.

Recommendations

This section provides recommendations that affect feature configuration.

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

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

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

VRF Scaling

By default, the system reserves VLAN IDs 4060 to 4094 for internal use. If you enable both the VRF scaling and the SPBM mode boot configuration flags, the system reserves additional VLAN IDs (3500 to 3998) for internal use.

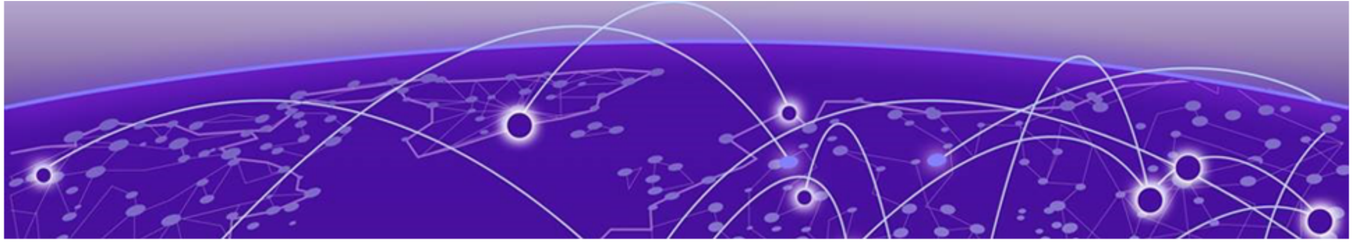
By default, VRF scaling is disabled and SPBM mode is enabled. When VRF scaling is disabled, you can have a maximum of 24 VRFs, depending on platform maximums.

The **`boot config flag vrf-scaling`** command does not apply to 4220 Series.

For the 5320 Series, only the following models support more than one VRF with IP configuration:

- 5320-16P-2MXT-2X
- 5320-24T-4X-XT
- 5320-24T-24S-4XE-XT
- 5320-48P-8XE
- 5320-48T-8XE

Of the preceding 5320 Series models, the **`boot config flag vrf-scaling`** command does not apply to 5320-16P-2MXT-2X or 5320-24T-4X-XT.



Important Notices

ExtremeCloud IQ Support on page 112
Compatibility with ExtremeCloud IQ Site Engine on page 112
Licensing on page 113
Memory Usage on page 113

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

ExtremeCloud IQ Support

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

For the most current information on switches supported by ExtremeCloud IQ, see ExtremeCloud™ IQ Release Notes.

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

The switch software integrates with ExtremeCloud IQ using IQAgent.

For more information, see *Fabric Engine User Guide*.

Compatibility with ExtremeCloud IQ Site Engine

To understand which versions of ExtremeCloud IQ Site Engine are compatible with this Network Operating System release on different hardware platforms, see Extended Firmware Support.

Licensing

Because the hardware supports more than one Network Operating System (NOS) personality, it uses a licensing scheme that is NOS agnostic.

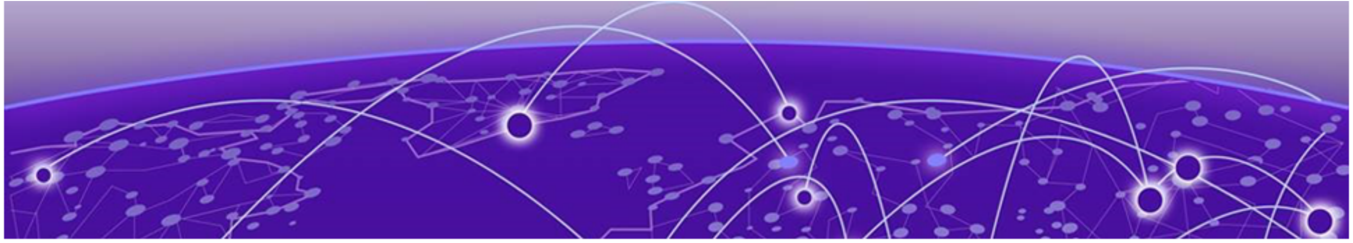
Table 42: Licensing model by platform

Platform	Model
4220 Series	The 4220 Series supports a subscription-licensing model that enables the Full CLI. These switches do not support an on-switch licensing model.
5000 Series 7x20 Series	The switches support an on-switch licensing model that includes Base, Premier, and MACsec licenses. Premier and MACsec licenses enable use of advanced features not available in the Base License. To see which features a platform supports, see *Fabric Engine and VOSS Feature Matrix*. Beginning with Fabric Engine 9.2 and ExtremeCloud IQ 25R2, ExtremeCloud IQ Site Engine 25.2.10, or Extreme Platform ONE, these switches are also subscription-license aware. Subscription licenses enable use of Premier features.

For more information about licensing including feature inclusion, order codes, and how to load a license file on the switch, see *Fabric Engine User Guide*.

Memory Usage

These switches intentionally reboot when memory usage on the switch reaches 95%.



Known Issues and Restrictions

Known Issues for this Release on page 114
Restrictions and Expected Behaviors on page 126

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

Known Issues for this Release

This section identifies the known issues in this release.

Issue number	Description	Workaround
	HTTPS connection fails for CA-signed certificate with certificate inadequate type error on FF.	Ensure End-Entity, Intermediate CA and Root CA certificates are all SHA256 based and RSA2048 key signed, and Extended key usage field is set to TLS webserver Auth only for subject and root. For intermediate, it must be set with other required bits to avoid this issue. Add the root, intermediate CAs in the trust store of the browser for accessing the EDM with HTTPS.
VOSS-1285	CAKs are not cleared after setting the device to factory-default.	None. Currently this is the default behavior and does not affect functionality of the MACsec feature.
VOSS-1289	On a MACsec-enabled port, you can see delayed packets when the MACsec port is kept running for more than 12 hours. This delayed packet counter can also increment when there is complete reordering of packets so that the application might receive a slow response. But in this second case, it is a marginal increase in the packet count, which occurs due to PN mismatch sometimes only during Key expiry, and does not induce any latency.	None.

Issue number	Description	Workaround
VOSS-1358	Traffic is forwarded to IGMP v2 SSM group, even after you delete the IGMP SSM-map entry for the group.	If you perform the delete action first, you can recreate the SSM-map record, and then disable the SSM-map record. The disabled SSM-map record causes the receiver to timeout because any subsequent membership reports that arrive and match the disabled SSM-map record are dropped. You can delete the SSM-map record after the receivers time out.
VOSS-1371	A large number of IPv6 VRRP VR instances on the same VLAN can cause high CPU utilization.	Do not create more than 10 IPv6 VRRP VRs on a single VLAN.
VOSS-1463 VOSS-1471	When you use Fabric Extend over IP (FE-IP) and Fabric Extend over Layer 2 VLAN (FE-VID) solution, if you change the ingress and egress .1p map, packets cannot follow correct internal QoS queues for FE tunnel to FE tunnel, or FE tunnel to regular NNI traffic.	Do not change the default ingress and egress .1p maps when using Fabric Extend. With default ingress and egress .1p maps, packets follow the correct internal QoS when using the Fabric Extend feature.
VOSS-1473	If the I-SID associated with a Switched UNI or Fabric Attach port does not have a platform VLAN association and you disable Layer 2 Trusted, then the non IP traffic coming from that port does not take the port QoS and still uses the .1p priority in the packet.	None.
VOSS-2014	IPv6 MLD Group is learned for Link-Local Scope Multicast Addresses. This displays additional entries in the Multicast routing tables.	None.

Issue number	Description	Workaround

VOSS-2033	The following error messages appear when you use the **`shutdown`** and **`no shutdown`** commands on the MLT interface with ECMP and BGP+ enabled:
	`CP1 [01/23/16 11:10:16.474:UTC] 0x00108628 00000000 GlobalRouter RCIP6 ERROR rcIpReplaceRouteNotifyIpv6:FAIL ReplaceTunnelRec conn_id 2`
	`CP1 [12/09/15 12:27:02.203:UTC] 0x00108649 00000000 GlobalRouter RCIP6 ERROR  ifyRpcOutDelFibEntry: del FIB of Ipv6Route failed with 0: ipv6addr: 201:6:604:0:0:0:0:0, mask: 96, nh: 0:0:0:0:0:0:0:0 cid 6657 owner BGP`
	`CP1 [12/09/15 12:20:30.302:UTC] 0x00108649 00000000 GlobalRouter RCIP6 ERROR  ifyRpcOutDelFibEntry: del FIB of Ipv6Route failed with 0: ipv6addr: 210:6:782:0:0:0:0:0, mask: 96, nh: fe80:0:0:0:b2ad:aaff:fe55:5088 cid 2361 owner OSPF`
		Disable the alternate path.

VOSS-2117	If you configure static IGMP receivers on an IGMPv3 interface and a dynamic join and leave are received on that device from the same destination VLAN or egress point, the device stops forwarding traffic to the static receiver group after the dynamic leave is processed on the device. The end result is that the IGMP static groups still exist on the device but traffic is not forwarded.	Disable and re-enable IGMP Snooping on the interface.
VOSS-2207	You cannot configure an SMTP server hostname that begins with a digit. The system displays the following error: `Error: Invalid IP Address or Hostname for SMTP server`	None.
VOSS-2208	While performing CFM Layer 2 traceroute between two BEBs using a transit BCB, the transit BCB hop is not seen, if the transit BCB has ISIS adjacencies over FE l3core with both source BEB and destination BEB.	None.
VOSS-2285	When on BEB, continuously pinging IPv6 neighbor address using CLI command **`ping -s`**, ping packets do not drop, but instead return no answer messages.	Restart the ping. Avoid intensive CPU processing.
VOSS-2333	Layer 2 ping to Virtual BMAC (VBMAC) fails, if the VBMAC is reachable using Layer 2 core.	None.
VOSS-4840	If you run the **`show fulltech`** command in an SSH session, do not disable SSH on the system. Doing so can block the SSH session.	None.

Issue number	Description	Workaround
VOSS-5331	When you enable FHS ND inspection on a VLAN, and an IPv6 interface exists on the same VLAN, the IPv6 host client does not receive a ping response from the VLAN.	None.
VOSS-5627	The system does not currently restrict the number of VLANs on which you can simultaneously configure NLB and Directed Broadcast, resulting in resource hogging.	Ensure that you configure NLB and Directed Broadcast on not more than 100 VLANs simultaneously, assuming one NLB cluster for each VLAN. Also, ensure that you configure NLB on a VLAN first, and then Directed Broadcast, so as to not exhaust the NLB and Directed Broadcast shared resources. The shared resources are NLB interfaces and VLANs with Directed Broadcast enabled. The permissible limit for the shared resources is 200.
VOSS-7139	DHCPv6 Snooping is not working in an SPB network as the DHCPv6 Snooping entries are not being displayed.	Administrator should add manual entries.
VOSS-7457	The switch can experience an intermittent traffic loss after you disable a Fabric Extend tunnel.	Bounce the tunnel between the devices.
VOSS-7472	EDM shows incorrect guidance for ACL TCP flag mask. EDM reports `0…63` as hexadecimal. CLI correctly shows `<0-0x3F | 0-63> Mask value <Hex | Decimal>`. This is a display issue only with no functional impact.	Use CLI to see the correct unit values.
VOSS-8424	A fragmented ping from an external device to a switch when the VLAN IP interface is tied to a non-default VRF fails.	None.
VOSS-10815	DvR over SMLT: Traffic is lost at failover on SMLT towards ExtremeXOS or Switch Engine switches. DvR hosts are directly connected to the DvR controllers vIST pair on SMLT LAG and switched-UNIs are dynamically added using Fabric Attach. Only occurs when the access SMLT is LACP MLT and all the ports in the MLT are down. When all ports in the MLT down and an ARP request is received over an NNI link, there is no physical port that can be associated with the ARP request. The ARP entry is learned against NNI link, and MAC syncs from vIST peer or from a non-vIST peer when bouncing vIST.	None.

Issue number	Description	Workaround
VOSS-11895	In a vIST SMLT environment where streams are both local and remote, if source and receiver port links are removed and reinserted several times, eventually traffic will not be forwarded to local single-homed receivers on one peer if the traffic is ingressing from the vIST peer over the NNI link. If the stream ingresses locally, it is received by the local UNI receivers.	Disable and re-enable Fabric Multicast (**`spbm <1-100> multicast enable`**) on the source VLAN to be able to delete the streams and come back in properly.
VOSS-11943	This release does not support per-port configuration of Application Telemetry. Because the feature is enabled globally and VSP 7432CQ supports 32 100 Gbps ports, an undesirable condition could be encountered when an exceeded amount of Application Telemetry mirrored packets are sent to the collector.	None.
VOSS-12330	When accessing the on-switch RESTCONF API documentation in a web browser, the page does not render correctly.	Ensure you include the trailing slash (/) in the URL: `http(s)://<ip-address>:8080/apps/restconfdoc/`. For more information, see *Fabric Engine User Guide*.
VOSS-13159	The ixgbevf Ethernet device driver within the TPVM does not correctly handle the interface MTU setting. Specifically, if you configure the interface in SR-IOV mode, packets larger than the MTU size are allowed.	To avoid this problem, configure the desired MTU size on both the relevant front-panel port and Insight port from the NOS CLI.
VOSS-13667	An intermittent issue in SMLT environments, where ARPs or IPv6 neighbors are resolved with delay can cause a transient traffic loss for the affected IPv6 neighbors. The situation auto-corrects.	None.
VOSS-13794	You cannot use SFTP to transfer files larger than 2 GB to the switch.	Use SCP.
VOSS-13904 VOSS-13932 VOSS-16503	VSP 4900 Series has 2 GB memory in a 64-bit system so the RESTCONF VLAN scaling number is smaller than on VSP 7400 Series, which has 16 GB physical memory. Using RESTCONF on VSP4900-48P or VSP4900-24S reduces the number of port-based VLANs on those platforms: • 2,000 for VSP4900-48P with RESTCONF • 1,000 for VSP4900-24S with RESTCONF	None.
VOSS-14597	Ping (originated from local CP) fails for jumbo frames on Layer 3 VSN interface.	None.
VOSS-15079	The Extreme Networks 10 meter SFP+ passive copper DAC (Model Number 10307) does not function on ports 2/3 and 2/4 of the VIM5-4X.	Use the Extreme Networks SFP+ active optical DAC (Model Number AA1403018-E6) with the VIM5-4X.

Issue number	Description	Workaround
VOSS-15391	An SNMP walk on the **`rcIgmpSnoopTraceTable`** table will fail with an **`OID not increasing`** error. CLI and EDM are unaffected by this issue.	None.
VOSS-15541	You can experience temporary traffic loss when shutting down an LACP SMLT port (and therefore causing the local SMLT to go down), in a network with scaled Multicast traffic over an SPB cloud, while the datapath processes all dpm letter messages during LCAP recovery. This slow LACP recovery situation is only seen with scaled Multicast traffic over an SPB cloud.	Use static MLTs.
VOSS-15812	Layer 3VSN IPv4 BGP (and static) routes having their next-hops resolved using IS-IS routes could result in traffic loss.	Choose the following workarounds, based on your deployment and needs: • Use static routes to reach the loopbacks used as BGP peers, (static routes having better preference than IS-IS); use static routes with next-hops reachable on the UNI side (L2VSN). • Use OSPF to reach the loopbacks used as BGP peers, but take care to ensure that the OSPF route towards the BGP peer is chosen as the “best route” (as IS-IS has a better preference than OSPF). There are several ways to accomplish this—either don’t redistribute that route in IS-IS if it is not needed, or control the redistribution with a route-map, etc. • Have BGP peers reachable directly using a C-VLAN; do not use loopback interfaces as BGP peer addresses. • If none of the workaround scenarios are suitable for your deployment, do not use internal Border Gateway Protocol (iBGP) peering.
VOSS-15878	VSP 4900 Series and VSP 7400 Series do not boot with just the serial console cable connected and no terminating device, for example, a terminal server, PC, or Mac.	Either attach terminal equipment or disconnect the console cable.

Issue number	Description	Workaround
VOSS-16971	On VSP4900-24S, VSP4900-24XE, andVSP4900-12MXU-12XE devices, and on the VIM5-4XE, if a copper SFP is plugged in with the cable inserted and the remote end is also plugged in, the peer box could see a link flap and take 6-8 seconds to link up.	First, plug in the SFP, and then insert the cable. The link up then happens in 3-4 seconds.
VOSS-18023	The management port on the 5520 Series switch does not support Auto-MDIX (the automatic detection of transmit and received twisted pairs). As a best practice, enable the default auto-negotiation setting on the management port. Because the management port does not support Auto-MDIX, when auto-negotiation is disabled, a crossover cable might be necessary to have the port link up and pass traffic. Note: If the peer device supports Auto-MDIX, then either a straight through or crossover will work. The issue occurs only if both ends of the connection do not support Auto-MDIX.	None.
VOSS-18238	When a management VLAN with DHCP is used to reach a RADIUS server, and the RADIUS server cannot be reached, the system waits for 15 minutes before attempting to reach the RADIUS server again. This is true even if the RADIUS server becomes reachable before the 15 minutes have elapsed.	None.
VOSS-18278	On the 5520 Series switch, when you make any change relating to port speed, the port statistics are cleared. This applies to all front panel fiber and copper ports as well as VIM ports. The following are examples of changes relating to port speed: • Changing the auto-negotiation configuration settings on a copper port • Different negotiated speed on a copper port • Changing out an optical device for one having a different speed, for example changing from 1 Gb to 10 Gb	None.
VOSS-19260	Port mirroring does not work on port 1/s1 of VSP 7400-48Y if the connection type is OVS/SR-IOV.	Use a connection type of VT-d for port 1/s1.
VOSS-19827	LLDP IPv6 neighbors do not display in EDM. LLDP IPv6 is only supported in CLI.	To display LLDP IPv6 neighbors, use the **`show lldp neighbor summary`** command.

Issue number	Description	Workaround
VOSS-20455	As the switch starts, it can display the following log messages due to incomplete initialization of the management stack when trying to send the first RADIUS packet: • `1 2021-02-17T23:32:16.810+01:00 DIST-H9-E3.1-01 CP1 - 0x000a45ae - 00000000 GlobalRouter RADIUS ERROR rad_sendRequest: unable to send a UDP packet. error 51, S_errno_ENETUNREACH` • `1 2021-02-17T23:32:16.811+01:00 DIST-H9-E3.1-01 CP1 - 0x000a45ac - 00000000 GlobalRouter RADIUS ERROR rad_processPendingRequest: unable to send request`	None. This issue has no functional impact.
VOSS-20456	Although the Management Router is not supported in the NOS, you can add a static route for VRF 512 using EDM. The route does not become active even if the next-hop address is reachable from the OOB management interface.	None. This issue has no functional impact.
VOSS-21097	In Multi-Area where vIST peers are boundary nodes, vIST can briefly flap during connection formation when IS-IS is disabled and then reenabled on both vIST peers.	None.
VOSS-21964	When using Windows SCP application on a switch to transfer a file, an error message displays even if a file transfers successfully.	
VOSS-22255	Ping, which originates from a local CP, fails for ICMP packets bigger than 1500 sent from Layer 3 VSN interface.	Initiate ping with packets size smaller than 1500.
VOSS-22522	RESTCONF is delayed in a scaled setup with 2,000 VLANs.	None.
VOSS-22858	LLDP neighbor should not be discovered with mismatch in MKA MACsec on 5520 Series ports.	Disable MKA on both sides or shut down the port on both sides.
VOSS-23146	Multi-area DvR/SPBM configuration: `Timeout: No response` message is returned during snmpwalk on one of the DvR controllers.	Run the snmpwalk command with an increased timeout. You can also run snmpwalk for a specific object.
VOSS-23181	When you enable the **`boot config flags macsec`** command, the indiscard counter increments on SPBM-enabled ports.	None. There is no functional impact.
VOSS-23216	If you do not enable the DvR interface when you configure a dvr-one-ip interface, the dvr-one-ip interface does not display when you issue the **`show dvr interfaces`** command.	Enable the DvR interface.

Issue number	Description	Workaround
VOSS-24777	In the following port configurations on 5520 Series, 5420 Series, VSP 4900 Series, and VSP 7400 Series, inVSN ACL entries match ingressing packets that have the same VID as the VLAN associated with the ACL I-SID even if the ACL inVSN I-SID is different: • on an S-UNI port without a platform VLAN • on a T-UNI port VLAN	None.
VOSS-24872	If the collector reachability path changes for Application Telemetry, it is not reflected properly in CLI. Packets remain mirrored towards the correct path but CLI does not reflect the next hop.	None. There is no functional impact.
VOSS-25023	5520 Series, 5420 Series, and 5320 Series platforms can reach 100% CPU utilization during inband transfer (FTP, SFTP, and SCP).	None.
VOSS-25162	RESTCONF ARP and MAC data: on 5x20 switches with 5K ARP entries and 5K MAC entries, it takes approximately 1 minute to retrieve data. The time increases based on the number of entries. The same occurs on VSP 7400 Series with over 15K entries.	None.
VOSS-25288	Secure boot information for 5720 Series, 7520 Series , and 7720 Series does not display when you issue the **`show sys-info`** command.	None.
VOSS-25728	You cannot assign a second disk to the second virtual service on the following switches: • VSP 4900 Series • VSP 7400 Series • 5720 Series	None.
VOSS-25874	Intermittent issue that causes inconsistency in show output.	None.
VOSS-25959	On the VSP 4900 Series, VSP 7400 Series, and 5720 Series, the virtual service does not operate properly when you configure *`e1000`* Network Interface Card (NIC) type for SR-IOV and VT-d connect types.	None.
VOSS-26028	On the VSP 4900 Series, VSP 7400 Series, and 5720 Series, the virtual service does not operate properly when you configure more than 16 virtual ports per Extreme Integrated Application Hosting port.	None.
VOSS-26032	NNI port remains in STP blocking state in a very specific scenario and configuration.	Bounce the NNI port.
VOSS-26099	MACsec Key Agreement (MKA) MACsec does not operate properly when you enable and disable MKA MACsec on the port 15-20 times.	None.

Issue number	Description	Workaround
VOSS-26122	Intermittently, some CLI commands related to sFlow functionality do not display in the CLI log.	None.
VOSS-26151	MACsec Key Agreement (MKA) does not operate between Fabric Engine 5520 Series and 5720 Series switches and ExtremeXOS 5520 Series and 5720 Series switches when you use GCM-AES-256 MACsec encryption cipher suite on copper ports.	As a workaround, use GCM-AES-128 MACsec encryption cipher suite to connect Fabric Engine 5520 Series and 5720 Series switches and Switch Engine 5520 Series and 5720 Series switches.
VOSS-26526	After you format a USB drive and issue the **`ls`** command, the current date and time does not display.	None.
VOSS-26527	Intermittently, the **`show sys-info`** command does not display the correct part number or serial number for the 2000 W AC PoE power supply (Model XN-ACPWR-2000W with front-to-back ventilation airflow).	None.
VOSS-26692	The entry for VLAN used to send/receive VXLAN packets to/from FIGW (for IPSec encapsulation) is missing from my_station_tcam table. In this case, traffic over the corresponding FE tunnel is lost.	Shut/no shut of the used sideband port fixes the problem.
VOSS-26822	Configuration tab for Ports 53-54 (VSP 7400-48Y) cannot be accessed from the first attempt.	Select menu options on your Mozilla Firefox browser. Alternatively, use another browser: Google Chrome, Safari, or Microsoft Edge.
VOSS-27235	If you delete a VLAN IP interface, the switch does not delete the associated DvR gateway IP address.	Manually delete the DvR gateway IP address.
VOSS-27643	On 5320 Series, packet port statistics do not increment for multicast traffic ingressing Layer 3 Fabric Extend NNI.	As a workaround, calculate the number of packets from the total number of bytes received.
VOSS-27784	Layer 3 VSN traffic continues to flow after you delete IP addresses in dual stack scenarios.	None.
VOSS-27875	On 7520-48XT-6C copper ports(1/1-1/48) with SLPP enabled, the port LED state is off.	None.
VOSS-28437	Layer 3 routed traffic is discarded in a square topology with two pairs of vIST DVR controllers in different domains when traffic should reach the diagonal switch.	As a workaround, save the configuration file with the NNI-MSTP flag configured and reboot the system.
VOSS-28241	For a routed Gigabit Ethernet interface, traffic doubles on vIST peers if you issue the **`action flushALL`** command.	None.
VOSS-28525	DHCP clients fail to receive an IP address in scenarios with VRRP over SMLT when SMLT goes down and the DHCP interface is configured to broadcast.	As a workaround, disable broadcast on the DHCP relay.

Issue number	Description	Workaround

VOSS-28625	Boundary Nodes return VRRP packets into the originating area and cause warning messages to display. The issue occurs if you create the following ACL rule on a Multi-area SPB Boundary Node:
	`filter acl 1 type inVsn matchType both`
	`filter acl i-sid 1 12990020`
	`filter acl ace 1 1`
	`filter acl ace action 1 1 permit monitor-isid-offset 1`
	`filter acl ace ethernet 1 1 ether-type eq ip`
	`filter acl ace 1 1 enable`
	The issue is caused by the interoperability of this specific ACL configured to mirror the I-SID traffic, and the Multi-area filters.
		Remove the ACL used to mirror I-SID traffic on the boundary node. Use Fabric RSPAN (Mirror to I-SID) to achieve similar functionality.
		Alternatively, use matchtype "uniOnly" instead of “both".

VOSS-28672	IPFIX does not learn MCoSPB NNI-UNI flows on 7520 Series, 7720 Series, and VSP 7400 Series.	None.
VOSS-29287	Interoperability issues can occur between VOSS/ Fabric Engine switches and ExtremeXOS/ Switch Engine switches when you use MACsec MKA and disable SCI tagging on both ends. Disabling SCI tagging on both ends works for ExtremeXOS/ Switch Engine if the VOSS/ Fabric Engine version is earlier than 8.7.	None.
VOSS-29711	If you enter a delayed reboot command for a device with at least one active RADIUS Accounting session, the switch does not send the RADIUS Accounting Stop or RADIUS Accounting Off packets, and console traces display on the screen.	None.
VOSS-30195	A potential LLDP flood issue can occur with certain third-party unmanaged devices on Auto-sense ports.	Eliminate the cause of flooding.
VOSS-30222	SSH connection is currently unavailable through Layer 2 FE Tunnel or Layer 3 FE Tunnel on the 5320 Series and 5420 Series.	Enable IPv6 Shortcuts.
VOSS-30287	An intermittent connectivity issue occurs over a Fabric Extend destination tunnel in a failover scenario when the IS-IS unicast FIB computation does not point to the shortest path.	This situation is temporary. You can perform an action, such as configuring any same I-SID on the Fabric Extend tunnel ends to trigger an IS-IS computation. Wait for the IS-IS computation to generate.
VOSS-30292	If IPv6 Shortcuts are explicitly disabled, SSH connections does not work on VSP 4900 Series.	Enable IPv6 Shortcuts.

Issue number	Description	Workaround
VOSS-30576	`WARNING: CPU: 0 PID: 1 at kernel/rcu/tree_plugin.h:297 rcu_note_context_switch+0x44/0x340` kernel message, which displays on the console during bootup has no functional impact on 4220 Series and 5320 SeriesXT. .	None.
VOSS-30980	After you enable an IP VPN instance on a VRF that you configure for the IS-IS logical interface and the adjacency establishes through the Fabric Extend tunnel with a nickname server, Dynamic Nickname Offers are discarded on the port with the Fabric Extend tunnel.	As a workaround, disable and then reenable IP VPN on the VRF or use the automatic nickname.
VOSS-30990	When you change the advanced-fabric-bandwidth-reservation flag from low to high, you cannot enable Auto-sense on ports reserved as loopback ports after you reboot the switch. An example of the message that displays is as follows: `Cleanup for auto-sense failed on port: 1/10, reason: VLAN cleanup failed!`	As a workaround, disable Auto-sense on reserved loopback ports before you reboot the switch.
VOSS-31315	The following message displays when you upgrade to VOSS Release 9.1 on VSP 4900 Series:`DMAR: [Firmware Bug]: No firmware reserved region can cover this RMRR [0x000000003e2e0000-0x000000003e2fffff], contact BIOS vendor for fixes.`	None.
VOSS-31352	When you disconnect a Fabric Attach client from an Auto-sense port and reconnect a device that does not transmit LLDP packets, the device displays the wrong port default VLAN ID when the port transitions from the WAIT to UNI state.	As a workaround, bring the port down and then bring the port up to restart the Auto-sense state on the switch to display the correct default VLAN ID when the port transitions to the UNI state.
VOSS-31465	When an IPv6 RSMLT in the forwarding state cannot ping the IPv6 link-local address of the vIST peer in that particular RSMLT VLAN, local routes whose next-hop is the link-local address of the vIST peer can fail.	None.
VOSS-31916	In some cases, when the Anycast GW router is configured on a vIST node or on a boundary node with at least two peer boundary nodes, pinging the Anycast GW IP does not work. Routing functionality, including next hop ARP resolution, is not affected.	None.

Issue number	Description	Workaround
VOSS-32147	ZTP+ fails to discover and connect to ExtremeCloud IQ Site Engine, in a scenario where two DNS servers are configured on the switch through DHCP but, although it is running, the primary DNS server cannot resolve the extremecontrol hostname.	In the DHCP server configuration, the primary DNS server must be able to resolve "extremecontrol". If one of the DNS servers cannot resolve the extremecontrol hostname, for example, in the case of a public DNS server, add that server in the DHCP configuration with a lower priority.
VOSS-32270	When ARP entries exceed the 8000 limit on VLANs without an assigned I-SID on 5520 Series, multiple error messages display and ARP entries fail to program correctly when you add additional ARP entries.	As a workaround, assign I-SIDs to VLANs that can manage more than 8000 ARP entries.
VOSS-32312	The following message displays on the console: `unable to rotate the file '/intflash/shared/telegraf.log', rename /intflash/shared/telegraf.log /intflash/shared/telegraf.<timestamp>.log: no such file or directory.`	None. You can safely ignore this message.
VOSS-32393	EDM displays an error when you configure the LLDP MED Tx TLV capabilities (**TLVsTxEnable)**.	Use CLI.
VOSS-32476	In a scenario with multiple misconfigurations in single and multiple areas such as Multi-area SPB inter-area duplicate nickname/system-ID recovery, log messages can be mismatched.	None.

Restrictions and Expected Behaviors

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

For Port Mirroring considerations and restrictions, see *Fabric Engine User Guide*.

General Restrictions and Expected Behaviors

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

Table 43: General restrictions

Issue number	Description	Workaround
—	If you access the Extreme Integrated Application Hosting virtual machine using **`virtual-service tpvm console`** and use the Nano text editor inside the console access, the command **`^o<cr>`** does not write the file to disk.	None.
VOSS-7	Even when you change the LLDP mode of an interface from CDP to LLDP, if the remote side sends CDP packets, the switch accepts them and refreshes the existing CDP neighbor entry.	Disable LLDP on the interface first, and then disable CDP and re-enable LLDP.
VOSS-687	EDM and CLI show different local preference values for a BGP IPv6 route. EDM displays path attributes as received and stored in the BGP subsystem. If the attribute is from an eBGP peer, the local preference displays as zero. CLI displays path attributes associated with the route entry, which can be modified by a policy. If a route policy is not configured, the local preference shows the default value of 100.	None.
VOSS-2166	The IPsec security association (SA) configuration has a NULL Encryption option under the **Encrpt-algo** parameter. Currently, you must fill the encrptKey and **keyLength** sub-parameters to set this option; however, these values are not used for actual IPsec processing as it is a NULL encryption option. The NULL option is required to interoperate with other vendors whose IPsec solution only supports that mode for encryption.	There is no functional impact due to this configuration and it only leads to an unnecessary configuration step. No workaround required.
VOSS-21946	When you create a vrf using the POSTMAN API platform, special characters, such as `\\\\` and `###` included in the URL are ignored.	None.

Table 43: General restrictions (continued)

Issue number	Description	Workaround
VOSS-5197	A BGP peer-group is uniquely identified by its name and not by its index. It is possible that the index that is configured for a peer-group changes between system reboots; however this has no functional impact.	None.
VOSS-7553	Option to configure the default queue profile rate-limit and weight values are inconsistent between EDM and CLI. Option to configure default values is missing in EDM.	None.
VOSS-7640	The same route is learned via multiple IPv6 routing protocols (a combination of two of the following : RIPng, OSPFv3 and BGPv6). In this specific case, an eBGP (current best – preference 45) route is replaced by and iBGP (preference 175) which in turn is replaced by and OSPFv3 (external 2) route (preference 125).	None.
VOSS-7647	With peer group configuration, you cannot configure Update Source interface with IPv6 loopback address in EDM.	Use CLI.
VOSS-9174	OVSDB remote VTEP and MAC details can take between 5 to 10 minutes to populate and display after a HW-VTEP reboots.	Known issue in VMware NSX 6.2.4. You can upgrade to NSX 6.4 to resolve this issue.
VOSS-9462	OVSDB VNID I-SID MAC bindings are not populated on HW-VTEPs after configuration changes.	Known issue in VMware NSX 6.2.4. You can upgrade to NSX 6.4 to resolve this issue.
VOSS-10168	The system CLI does not prevent you from using the same IP address for the VXLAN Gateway hardware VTEP replication remote peer IP and OOB Management IP.	Manually check the IP configured as the OOB Management IP. Do not use the OOB Management IP address as the replication remote peer IP address.

Table 43: General restrictions (continued)

Issue number	Description	Workaround
VOSS-11817	The OVS connect-type for virtual service Vports is designed in such a way that it connects to any generic virtual machine (VM) guest OS version using readily available Ethernet device drivers. This design approach provides initial connectivity to the VM in a consistent manner. A consequence of this approach is that Vports created with connect-type OVS will show up as 1 Gbps interfaces in the VM even though the underlying Ethernet connection supports 10 Gbps .	If additional performance is desired, upgrade the VM guest OS with an Ethernet device driver that supports 10 Gbps interfaces.
VOSS-12151	If logical switch has only hardware ports binding, and not VM behind software VTEP, Broadcast, Unknown Unicast, and Multicast (BUM) traffic does not flow between host behind two hardware VTEP. The NSX replicator node handles the BUM traffic. NSX does not create the replicator node unless a VM is present. In an OVSDB topology, it is expected that at least one VM connects to the software VTEP. This issue is an NSX-imposed limitation.	After you connect the VM to the software VTEP, the issue is not seen.
VOSS-17871	Starting with VOSS 8.1.5, internal system updates have resulted in a more accurate accounting of memory utilization. This can result in a higher baseline memory utilization reported although actual memory usage is not impacted.	Update any network management alarms that are triggered by value with the new baseline.
VOSS-18523	When you configure a port using Zero Touch Provisioning Plus (ZTP+) with ExtremeCloud IQ Site Engine, the port cannot be part of both a tagged VLAN and an untagged VLAN.	n/a

Table 43: General restrictions (continued)

Issue number	Description	Workaround
VOSS-18851	Do not define a static route in which the NextHop definition uses an Inter-VRF redistributed route. Such a definition would require the system to perform a double lookup. When you attempt to define a static route in this way, an error message is generated.	Define the static route in such a way that it does not require Inter-VRF redistributed routing.
VOSS-21620	When interior nodes are running software earlier than Release 8.4 and a Multi-area takeover occurs between the boundary nodes (when the non-designated boundary node transitions to designated) in the network, the interior nodes might detect a false duplicate case between the stale LSP of the old virtual node and the new virtual node. This has no functional impact in the network.	n/a
wi01068569	The system displays a warning message that routes will not inject until the apply command is issued after the enable command. The warning applies only after you enable redistribution, and not after you disable redistribution. For example: **`Switch:1(config)#isis apply redistribute direct vrf 2`**	n/a
wi01112491	IS-IS enabled ports cannot be added to an MLT. The current release does not support this configuration.	n/a

Table 43: General restrictions (continued)

Issue number	Description	Workaround
wi01122478	Stale SNMP server community entries for different VRFs appear after reboot with no VRFs. On a node with a valid configuration file saved with more than the default vrf0, SNMP community entries for that VRF are created and maintained in a separate text file, `snmp_comm.txt`, on every boot. The node reads this file and updates the SNMP communities available on the node. As a result, if you boot a configuration that has no VRFs, you can still see SNMP community entries for VRFs other than the globalRouter vrf0 .	n/a
wi01137195	A static multicast group cannot be configured on a Layer 2 VLAN before enabling IGMP snooping on the VLAN. After IGMP snooping is enabled on the Layer 2 VLAN for the first time, static multicast group configuration is allowed, even when IGMP snooping is disabled later on that Layer 2 VLAN.	n/a
wi01141638	When a VLAN with 1000 multicast senders is deleted, the console or Telnet session stops responding and SNMP requests time out for up to 2 minutes.	n/a

Table 43: General restrictions (continued)

Issue number	Description	Workaround
wi01142142	When a multicast sender moves from one port to another within the same BEB or from one vIST peer BEB to another, with the old port operationally up, the source port information in the output of the **show ip igmp sender** command is not updated with new sender port information.	You can perform one of the following workarounds: • On an IGMP snoop-enabled interface, you can flush IGMP sender records. Caution: Flushing sender records can cause a transient traffic loss. • On an IGMP-enabled Layer 3 interface, you can toggle the IGMP state. Caution: Expect traffic loss until IGMP records are built after toggling the IGMP state.
wi01171670	Telnet packets get encrypted on MACsec-enabled ports.	None.
wi01210217	The command **show eapol auth-stats** displays `LAST-SRC-MAC` for NEAP sessions incorrectly.	n/a
wi01212034	When you disable EAPoL globally: • Traffic is allowed for static MAC configured on EAPoL enabled port without authentication. • Static MAC config added for authenticated NEAP client is lost.	n/a
wi01212247	BGP tends to have many routes. Frequent additions or deletions impact network connectivity. To prevent frequent additions or deletions, reflected routes are not withdrawn from client 2 even though they are withdrawn from client 1. Disabling route-reflection can create a black hole in the network.	Bounce the BGP protocol globally.
wi01212585	LED blinking in EDM is representative of, but not identical to, the actual LED blinking rates on the switch.	n/a
wi01213066 wi01213374	EAP and NEAP are not supported on brouter ports.	n/a

Table 43: General restrictions (continued)

Issue number	Description	Workaround
wi01213336	When you configure tx mode port mirroring on T-UNI and SPBM NNI ports, unknown unicast, broadcast and multicast traffic packets that ingress these ports appear on the mirror destination port, although they do not egress the mirror source port. This is because tx mode port mirroring happens on the mirror source port before the source port squelching logic drops the packets at the egress port.	n/a
wi01219658	The command **`show khi port-statistics`** does not display the count for NNI ingress control packets going to the CP.	n/a
wi01219295	SPBM QOS: Egress UNI port does not follow port QOS with ingress NNI port and Mac-in-Mac incoming packets.	n/a
wi01223526	ISIS logs duplicate system ID only when the device is a direct neighbor.	n/a
wi01223557	Multicast outage occurs on LACP MLT when simplified vIST peer is rebooted.	You can perform one of the following workarounds: • Enable PIM on the edge. • Ensure that IST peers are either RP or DR but not both.
wi01224683 wi01224689	Additional link bounce can occur on 10 Gbps ports when toggling links or during cable re-insertion. Additional link bounce can occur with 40 Gbps optical cables and 40 Gbps break-out cables, when toggling links or during cable re-insertion.	n/a
wi01229417	Origination and termination of IPv6 6-in-4 tunnel is not supported on a node with vIST enabled.	None.

Table 43: General restrictions (continued)

Issue number	Description	Workaround
wi01232578	When SSH keyboard-interactive-auth mode is enabled, the server generates the password prompt to be displayed and sends it to the SSH client. The server always sends an expanded format of the IPv6 address. When SSH keyboard-interactive-auth mode is disabled and password-auth is enabled, the client itself generates the password prompt, and it displays the IPv6 address format used in the **ssh** command.	None.
VOSS-26218	In a scaled environment, running the **show io l2-tables** command reiteratively can cause the switch to reboot.	For scaled scenarios, do not run the **show io l2-tables** command in a loop.
VOSS-31214	With the upgrade to Mocana 7, RadSec Proxy certificates must conform to the following SP 800-132 specifications for PBKDFv2 parameters: • salt length of at least 128 bits • derived key length of at least 112 bits • iteration count of at least 1000 When you generate public or private key-pairs protected by a password with older versions of OpenSSL, the default PKCS5_SALT_LEN is 8 bytes, which results in TLS failures.	You can perform one of the following workarounds: • Recompile OpenSSL to use a PKCS5_SALT_LEN value of 16 bytes and generate new certificates. • Use a newer version of OpenSSL that is FIPS approved. • Generate the keys without password protection.

Filter Restrictions

The following table identifies known restrictions.

Table 44: ACL restrictions

Applies To	Restriction
All platforms	Only port-based ACLs are supported on egress. VLAN-based ACLs are not supported.
All platforms	IPv6 ingress and IPv6 egress QoS ACL/filters are not supported. **Note:** IPv6 ACL DSCP Remarking is supported.
All platforms	Control packet action is not supported on InVSN Filter or IPv6 filters generally.

Table 44: ACL restrictions (continued)

Applies To	Restriction
All platforms	IPv4/IPv6 VLAN based ACL filters will be applied on traffic received on all the ports if it matches VLAN ID associated with the ACL.
All platforms	Scaling numbers are reduced for IPv6 filters.
All platforms	The InVSN Filter does supports IP Shortcut traffic only on both UNI and NNI ports, but does not support IP Shortcut traffic on UNI ports only and NNI ports only.
All platforms	The InVSN Filter does not filter packets that arrive on NNI ingress ports but are bridged to other NNI ports or are for transit traffic.
All platforms	You can insert an InVSN ACL type for a Switched UNI only if the Switched UNI I-SID is associated with a platform VLAN.

Table 45: ACE restrictions

Applies To	Restriction
All platforms	When an ACE with action count is disabled, the statistics associated with the ACE are reset.
All platforms	Only security ACEs are supported on egress. QoS ACEs are not supported.
All platforms	ICMP type code qualifier is supported only on ingress filters.
All platforms	For port-based ACLs, you can configure VLAN qualifiers. Configuring port qualifiers are not permitted.
All platforms	For VLAN-based ACLs, you can configure port qualifiers. Configuring VLAN qualifiers are not permitted.
All platforms	Egress QoS filters are not supported for IPv6 filters.
All platforms	Source/Destination MAC addresses cannot be added as attributes for IPv6 filters ACEs.

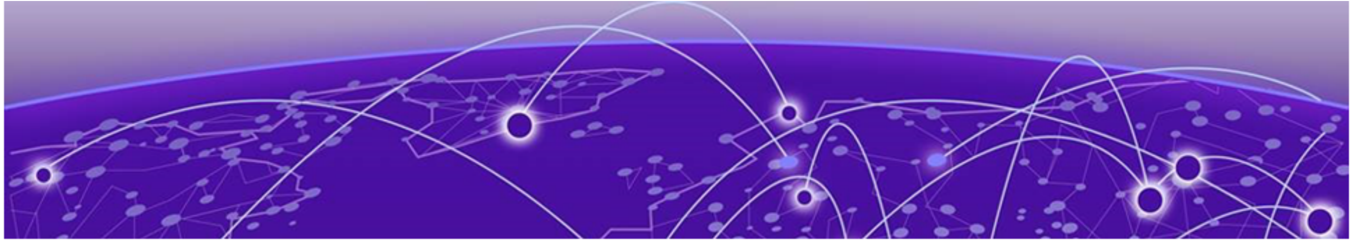
Resolved Issues this Release

This release incorporates all fixes from prior releases, up to and including the following releases:

- Fabric Engine 8.10.6.1
- Fabric Engine 9.0.5.1
- Fabric Engine 9.1.1.0

Issue number	Description
CFD-11008	Voss - DVR- After upgrading core and edge to 8.10.3.0 persistent incorrect entries remain in HW/SW.
CFD-11673	5720 crash with core file.
CFD-11824	VSP 7400.8.10.1.0 Dropping ARP reply packet and other unicast for UNI and unicast when ingresses NNI destined for itself when ingressing in different VLAN, and needs to be bridged out to the destined VLAN using hairpin.
CFD-11947	Fabric Engine – End-Devices unreachable from some sources in the network in association with ARP entries pointing to TX-NNI.
CFD-11988	5520: Segmented Management VLAN not working after upgrade to 9.0.2.0.
CFD-12011	5320 - 9.0.3.0 - Lifecycle Crash Reporter: Process Name: ssio, Thread Name: main, Signal: 6, Slot: 1, PID 2878, LWP: 2878.
CFD-12194	VOSS: 9.0.3.0 - Switch IP interfaces are not reachable after migrating Layer 3 to VSP 7400s.
CFD-12450	7520: ping fails to MGMT CLIP even from the vIST peer.
CFD-12503	5320 (9.0.3.0) - False alarm regarding no PSU redundancy reported on ExtremeCloud IQ Site Engine.
CFD-12572	ISIS Multiarea: duplication of packets on management VLAN seen on ABR.
CFD-12609	Port Where ARP Is Learned Is Stuck In TX-NNI State Until Port Is Bounced.
CFD-12691	VOSS 9.0.3 - no connectivity out of VLAN, TX-NNI.
CFD-12830	Port PoE status is OtherFault on 5420F after upgrading to v9.0.4.0 and recovers after reboot.
CFD-12852	VOSS - 8.10.5.0 - Access switch becomes unreachable after period of time - TX-NNI.

Issue number	Description
CFD-12923	Incorrect virtual-service mem-size.
CFD-12952	7520-48Y-8C: "Message-Authenticator" attribute with CoA.
CFD-13075	5420 - After upgrading to 9.1, generating lcdMacAndMacPortToPimPort in the logs.
CFD-13244	ctAliasMacAddressTime being reported in seconds instead of timeticks for sysUpTime.
VOSS-21123	Brouters on UNIs of VSP 7400 vIST peers cannot ping each other.
VOSS-30903	The following message displays temporarily when you configure your switch from Zero Touch Provisioning mode to SPBM mode: `COP-SW INFO Impossible case counter = 1, Thread ID = 2601, l2addr_tail = 3, l2addr_head = 4, Invalid MIM port = 1073741830 vid = 4051 MAC Addr = b0:27:cf:43:44:8c Operation = 1`
VOSS-31145	When you configure Anycast IP Gateway in a Multi-area SPBM network with four boundary nodes of different platform types, an intermittent issue occurs where an ARP entry points towards TX-NNI instead of the proper NNI.
VOSS-31226	In a Multi-area SPBM network with four boundary nodes, virtual links can remain down when you disable IS-IS remote adjacencies on each boundary node.
VOSS-31763	When you enable MACsec on the 5520 Series VIM port, the link goes down and comes back up.
VOSS-31814	A duplicate timestamp displays when you issue the **`show io l2-tables`** or **`show io l3-tables`** commands.



Related Information

MIB Changes on page 138

MIB Changes

Deprecated MIBs

Table 46: Common

Object Name	Object OID	Deprecated in Release
rcIpBgpGeneralGroupRoutePolicyIn	1.3.6.1.4.1.2272.1.8.101.1.22	8.5
rcIpBgpGeneralGroupRoutePolicyOut	1.3.6.1.4.1.2272.1.8.101.1.23	8.5
rcIpConfOspfRfc1583Compatibility	1.3.6.1.4.1.2272.1.8.1.4.5	8.5
rcDvrBackboneEntriesArea	1.3.6.1.4.1.2272.1.219.8.1.12	9.0
rcDvrBackboneMemberArea	1.3.6.1.4.1.2272.1.219.9.1.6	9.0
rcDvrBackboneMultiAreaVnodeEntriesArea	1.3.6.1.4.1.2272.1.219.10.1.12	9.0

Modified MIBs

Table 47: Common

Object Name	Object OID	Modified in Release	Modification
rcIpAdEntIfType	1.3.6.1.4.1.2272.1.8.2.1.10	9.0.3	CHANGE: index MAX-ACCESS level: from read-only to read-write rcIpAdEntIfType 1.3.6.1.4.1.2272.1.8.2.1.10 OTHER: Update description to include the new values added to enum
rcDigitalCertificateSubjectPublicKey	1.3.6.1.4.1.2272.1.222.1.1.8.1.11	9.1	CHANGE_RANGE: Changed the range from 0..2048 to 0..8192
rcDigitalCertificateStoreSubjectPublicKey	1.3.6.1.4.1.2272.1.222.1.1.9.1.13	9.1	CHANGE_RANGE: Changed the range from 0..4096 to 0..8192
rcDigitalCertificateKeySize	1.3.6.1.4.1.2272.1.222.1.1.10.1.3	9.1	CHANGE_TYPE: Changed the type from Integer32 to INTEGER
rcDigitalCertificateKeySize	1.3.6.1.4.1.2272.1.222.1.1.10.1.3	9.1	CHANGE_RANGE: Changed the range from 2048 to 1024..8192
rcRateLimitIfTrafficType	1.3.6.1.4.1.2272.1.14.14.1.2	9.1	ADD_NEW_VALUE: unknown-unicast(4)
rcDigitalCertSubjectPublicKey	1.3.6.1.4.1.2272.1.222.1.1.4.1.11	9.1	CHANGE_RANGE: Changed the range from 0..2048 to 0..8192
rcDigitalCertStoreSubjectPublicKey	1.3.6.1.4.1.2272.1.222.1.1.5.1.12	9.1	CHANGE_RANGE: Changed the range from 0..4096 to 0..8192
rcIpNewRoutePrefProtocol	1.3.6.1.4.1.2272.1.8.100.30.1.2	9.1	ADD_NEW_VALUE: isisExternal(14)
rcSysLocatorLED	1.3.6.1.4.1.2272.1.1.125	9.1	OTHER: Update description to include 5720
rcPortType	1.3.6.1.4.1.2272.1.4.10.1.1.2	9.1	ADD_ENUM: 251-256
rcVossSystemCardLedStatus	1.3.6.1.4.1.2272.1.101.1.1.5.1.4	9.1	ADD_NEW_VALUE: greenSteadyAmberBlinking(10)
rcVossSystemCardLedStatus	1.3.6.1.4.1.2272.1.101.1.1.5.1.4	9.1	ADD_NEW_VALUE: greenSteadyGreenBlinking(11)
rcVossSystemCardLedStatus	1.3.6.1.4.1.2272.1.101.1.1.5.1.4	9.1	ADD_NEW_VALUE: amberSteadyAmberBlinking(12)

Table 47: Common (continued)

Object Name	Object OID	Modified in Release	Modification
rcVossSystemCardLedStatus	1.3.6.1.4.1.2272.1.101.1.1.5.1.4	9.1	ADD_NEW_VALUE: amberSteadyGreenBlinking(13)
rcVossSystemCardLedStatus	1.3.6.1.4.1.2272.1.101.1.1.5.1.4	9.1	Other: Update description to show that the new values are available only on 4220
rcMltName	1.3.6.1.4.1.2272.1.17.10.1.2	9.1	CHANGE_RANGE: Changed the range from 0..20 to 0..64
rcRadiusServHostAddress	1.3.6.1.4.1.2272.1.29.5.1.2	9.1	CHANGE_RANGE: restricted to 113 characters length due to the max OID length
SnpxChassisType		9.1	OTHER: Platform Display changed for: 5320-24T-24S-4XE-XT-FabricEngine and 5320-24T-4X-XT-FabricEngine
rcChasType	1.3.6.1.4.1.2272.1.4.1	9.1	OTHER: Chassis type changed for 5320-24T-24S-4XE-XT-FabricEngine and 5320-24T-4X-XT-FabricEngine
rc2kCardFrontType	1.3.6.1.4.1.2272.1.100.6.1.2	9.1	OTHER: Card front type changed for 5320-24T-24S-4XE-XT-FabricEngine and 5320-24T-4X-XT-FabricEngine
rcNlsMgmtInstanceId	.1.3.6.1.4.1.2272.1.223.1.1.1	9.1	ADD_NEW_VALUE: sdwan(5)
rcNlsMgmtInterfaceType	.1.3.6.1.4.1.2272.1.223.1.1.2	9.1	ADD_NEW_VALUE: sdwan(5)
rcNlsMgmtAddrInstanceId	.1.3.6.1.4.1.2272.1.223.2.1.1	9.1	ADD_NEW_VALUE: sdwan(5)
rcNlsMgmtNetInstance	.1.3.6.1.4.1.2272.1.223.3.1.2	9.1	ADD_NEW_VALUE: sdwan(5)
rcNlsMgmtIpv6neighborInstance	.1.3.6.1.4.1.2272.1.223.4.1.2	9.1	ADD_NEW_VALUE: sdwan(5)
rcNlsMgmtStatsInstance	.1.3.6.1.4.1.2272.1.223.7.1.1	9.1	ADD_NEW_VALUE: sdwan(5)

Table 47: Common (continued)

Object Name	Object OID	Modified in Release	Modification
rcNlsMgmtIpRouteInstance	.1.3.6.1.4.1.2272.1.223.8.1.4	9.1	ADD_NEW_VALUE: sdwan(5)
rcNlsMgmtIpv6RouteInstance	.1.3.6.1.4.1.2272.1.223.9.1.4	9.1	ADD_NEW_VALUE: sdwan(5)
rcNlsMgmtIPv4AddressInstanceId	.1.3.6.1.4.1.2272.1.223.12.1.1	9.1	ADD_NEW_VALUE: sdwan(5)
rcNlsMgmtIPv6AddressInstanceId	.1.3.6.1.4.1.2272.1.223.13.1.1	9.1	ADD_NEW_VALUE: sdwan(5)
rcNlsMgmtKhiStatsInstanceId	.1.3.6.1.4.1.2272.1.223.21.1.1	9.1	ADD_NEW_VALUE: sdwan(5)
rcNlsMgmtDhcpClient	.1.3.6.1.4.1.2272.1.223.23.1	9.1	CHANGE_RANGE: move cycle from 5 --> 19, move disable from 6 --> 20
rcNlsMgmtDhcpClientPreferredInterface	.1.3.6.1.4.1.2272.1.223.23.2	9.1	CHANGE_RANGE: move none from 6 --> 20
rcSshKeyExchangeMethod	1.3.6.1.4.1.2272.1.34.1.23	9.1	ADD_NEW_VALUE: diffieHellmanGroup14Sha256(3)
rcSshKeyExchangeMethod	1.3.6.1.4.1.2272.1.34.1.23	9.1	ADD_NEW_VALUE: diffieHellmanGroup16Sha512(4)
rcSshKeyExchangeMethod	1.3.6.1.4.1.2272.1.34.1.23	9.1	ADD_NEW_VALUE: diffieHellmanGroup18Sha512(5)
rcIpAdEntIfType	.1.3.6.1.4.1.2272.1.8.2.1.10	9.1	ADD_NEW_VALUE: mgmtSdwan(9)
rcIpv6AddressIfType	.1.3.6.1.4.1.2272.1.62.1.1.3.1.13	9.1	ADD_NEW_VALUE: mgmtSdwan(7)
rcSysMTUSize	1.3.6.1.4.1.2272.1.1.55	9.2	ADD ENUM: mtu9416(5)
rcVossSystemTemperatureSensorDescription	1.3.6.1.4.1.2272.1.101.1.1.2.1.2	9.2	CHANGE_RANGE: Changed from DisplayString (SIZE (0..20)) to DisplayString (SIZE (0..30))
rcAutoSenseMultihostMacMax	1.3.6.1.4.1.2272.1.231.1.1.1.24	9.2	OTHER: default value 2 -> 4
rcAutoSenseMultihostEapMacMax	1.3.6.1.4.1.2272.1.231.1.1.1.25	9.2	OTHER: default value 2 -> 4
rcAutoSenseMultihostNonEapMacMax	1.3.6.1.4.1.2272.1.231.1.1.1.26	9.2	OTHER: default value 2 -> 4

Table 47: Common (continued)

Object Name	Object OID	Modified in Release	Modification
rcPortAutoSenseState	1.3.6.1.4.1.2272.1.4.10.1.1.134	9.2	OTHER: renamed uniOnboarding(4) -> uni(4) ADD_ENUM: nniMlt(20) ADD_ENUM: nniMltIsisUp(21) ADD_ENUM: nniMltOnboarding(22) ADD_ENUM: nniMltAuthFail(23) OTHER: renamed nniOnboading(10) -> nniOnboarding(10)
rcPortType	1.3.6.1.4.1.2272.1.4.10.1.1.2	9.2	

Table 48: 4220 Series

Object Name	Object OID	Modified in Release	Modification
bspePethPsePortPowerClassifications	1.3.6.1.4.1.45.5.8.1.1.1.15	9.2	OTHER: Update description to include 4220 platform
rc2kBootConfigAdvancedFeatureBwReservation	1.3.6.1.4.1.2272.1.100.5.1.51	9.2	OTHER: Update description to include the new values for 4220-8X, 4220-4MW-8P-4X and 4220-4MW-20P-4X

Table 49: 5320 Series

Object Name	Object OID	Modified in Release	Modification
rcLicenseLicenseType	1.3.6.1.4.1.2272.1.56.4	9.1	Added Enum: ep1Advanced(28), ep1Standard(29), pilot(30), ep1AdvancedPlusMacsec(31), ep1StandardPlusMacsec(32), pilotPlusMacsec(33), ep1AdvancedPlusPremier(34), ep1AdvancedPlusPremierPlusMacsec(35), ep1StandardPlusPremier(36),

Table 49: 5320 Series (continued)

Object Name	Object OID	Modified in Release	Modification
			ep1StandardPlusPremierPlusMacsec(37), pilotPlusPremier(38), pilotPlusPremierPlusMacsec(39)
rcIpRedistributeInterVrfSetTag	1.3.6.1.4.1.2272.1.8.100.22.1.9	9.1	CHANGE_TYPE: From Interger32 to Unsigned32
rcBridgeTpFdbStatus	1.3.6.1.4.1.2272.1.14.20.1.3	9.1	ADD_ENUM: anycast(9)
rcBridgeIsidFdbStatus	1.3.6.1.4.1.2272.1.14.23.1.3	9.1	ADD_ENUM: anycast(9)
rc2kBootConfigAdvancedFeatureBwReservation	1.3.6.1.4.1.2272.1.100.5.1.51	9.2	OTHER: Update description to include the new values for new models

Table 50: 5420 Series

Object Name	Object OID	Modified in Release	Modification
rcLicenseLicenseType	1.3.6.1.4.1.2272.1.56.4	9.1	Added Enum: ep1Advanced(28), ep1Standard(29), pilot(30), ep1AdvancedPlusMacsec(31), ep1StandardPlusMacsec(32), pilotPlusMacsec(33), ep1AdvancedPlusPremier(34), ep1AdvancedPlusPremierPlusMacsec(35), ep1StandardPlusPremier(36), ep1StandardPlusPremierPlusMacsec(37), pilotPlusPremier(38), pilotPlusPremierPlusMacsec(39)
rcIpRedistributeInterVrfSetTag	1.3.6.1.4.1.2272.1.8.100.22.1.9	9.1	CHANGE_TYPE: From Interger32 to Unsigned32

Table 50: 5420 Series (continued)

Object Name	Object OID	Modified in Release	Modification
rcBridgeTpFdbStatus	1.3.6.1.4.1.2272.1.14.20.1.3	9.1	ADD_ENUM: anycast(9)
rcBridgeIsidFdbStatus	1.3.6.1.4.1.2272.1.14.23.1.3	9.1	ADD_ENUM: anycast(9)

Table 51: 5520 Series

Object Name	Object OID	Modified in Release	Modification
rcLicenseLicenseType	1.3.6.1.4.1.2272.1.56.4	9.1	Added Enum: ep1Advanced(28), ep1Standard(29), pilot(30), ep1AdvancedPlusMacsec(31), ep1StandardPlusMacsec(32), pilotPlusMacsec(33), ep1AdvancedPlusPremier(34), ep1AdvancedPlusPremierPlusMacsec(35), ep1StandardPlusPremier(36), ep1StandardPlusPremierPlusMacsec(37), pilotPlusPremier(38), pilotPlusPremierPlusMacsec(39)
rcIpRedistributeInterVrfSetTag	1.3.6.1.4.1.2272.1.8.100.22.1.9	9.1	CHANGE_TYPE: From Interger32 to Unsigned32
rcBridgeTpFdbStatus	1.3.6.1.4.1.2272.1.14.20.1.3	9.1	ADD_ENUM: anycast(9)
rcBridgeIsidFdbStatus	1.3.6.1.4.1.2272.1.14.23.1.3	9.1	ADD_ENUM: anycast(9)

Table 52: 5720 Series

Object Name	Object OID	Modified in Release	Modification
rcLicenseLicenseType	1.3.6.1.4.1.2272.1.56.4	9.1	Added Enum: ep1Advanced(28), ep1Standard(29), pilot(30), ep1AdvancedPlusMacsec(31), ep1StandardPlusMacsec(32), pilotPlusMacsec(33), ep1AdvancedPlusPremier(3

Table 52: 5720 Series (continued)

Object Name	Object OID	Modified in Release	Modification
			4), ep1AdvancedPlusPremierPlusMacsec(35), ep1StandardPlusPremier(36), ep1StandardPlusPremierPlusMacsec(37), pilotPlusPremier(38), pilotPlusPremierPlusMacsec(39)
rcIpRedistributeInterVrfSetTag	1.3.6.1.4.1.2272.1.8.100.22.1.9	9.1	CHANGE_TYPE: From Interger32 to Unsigned32
rcBridgeTpFdbStatus	1.3.6.1.4.1.2272.1.14.20.1.3	9.1	ADD_ENUM: anycast(9)
rcBridgeIsidFdbStatus	1.3.6.1.4.1.2272.1.14.23.1.3	9.1	ADD_ENUM: anycast(9)

Table 53: 7520 Series

Object Name	Object OID	Modified in Release	Modification
rcLicenseLicenseType	1.3.6.1.4.1.2272.1.56.4	9.1	Added Enum: ep1Advanced(28), ep1Standard(29), pilot(30), ep1AdvancedPlusMacsec(31), ep1StandardPlusMacsec(32), pilotPlusMacsec(33), ep1AdvancedPlusPremier(34), ep1AdvancedPlusPremierPlusMacsec(35), ep1StandardPlusPremier(36), ep1StandardPlusPremierPlusMacsec(37), pilotPlusPremier(38), pilotPlusPremierPlusMacsec(39)
rcIpRedistributeInterVrfSetTag	1.3.6.1.4.1.2272.1.8.100.22.1.9	9.1	CHANGE_TYPE: From Interger32 to Unsigned32

Table 53: 7520 Series (continued)

Object Name	Object OID	Modified in Release	Modification
rcBridgeTpFdbStatus	1.3.6.1.4.1.2272.1.14.20.1.3	9.1	ADD_ENUM: anycast(9)
rcBridgeIsidFdbStatus	1.3.6.1.4.1.2272.1.14.23.1.3	9.1	ADD_ENUM: anycast(9)

Table 54: 7720 Series

Object Name	Object OID	Modified in Release	Modification
rcLicenseLicenseType	1.3.6.1.4.1.2272.1.56.4	9.1	Added Enum: ep1Advanced(28), ep1Standard(29), pilot(30), ep1AdvancedPlusMacsec(31), ep1StandardPlusMacsec(32), pilotPlusMacsec(33), ep1AdvancedPlusPremier(34), ep1AdvancedPlusPremierPlusMacsec(35), ep1StandardPlusPremier(36), ep1StandardPlusPremierPlusMacsec(37), pilotPlusPremier(38), pilotPlusPremierPlusMacsec(39)
rcIpRedistributeInterVrfSetTag	1.3.6.1.4.1.2272.1.8.100.22.1.9	9.1	CHANGE_TYPE: From Interger32 to Unsigned32
rcBridgeTpFdbStatus	1.3.6.1.4.1.2272.1.14.20.1.3	9.1	ADD_ENUM: anycast(9)
rcBridgeIsidFdbStatus	1.3.6.1.4.1.2272.1.14.23.1.3	9.1	ADD_ENUM: anycast(9)

New MIBs

Table 55: Common

Object Name	Object OID	New in Release
rcIsisLogicalInterfaceMAVirtualLink	1.3.6.1.4.1.2272.1.63.26.1.35	9.0.3
rcLldpXMedLocMediaPolicyTable	1.3.6.1.4.1.2272.1.220.1.2.5	9.0.3
rcLldpXMedLocMediaPolicyLocalPortNum	1.3.6.1.4.1.2272.1.220.1.2.5.1.1	9.0.3
rcLldpXMedLocMediaPolicyAppType	1.3.6.1.4.1.2272.1.220.1.2.5.1.2	9.0.3

Table 55: Common (continued)

Object Name	Object OID	New in Release
rcLldpXMedLocMediaPolicyVlanID	1.3.6.1.4.1.2272.1.220.1.2.5.1.3	9.0.3
rcLldpXMedLocMediaPolicyPriority	1.3.6.1.4.1.2272.1.220.1.2.5.1.4	9.0.3
rcLldpXMedLocMediaPolicyDscp	1.3.6.1.4.1.2272.1.220.1.2.5.1.5	9.0.3
rcLldpXMedLocMediaPolicyRowStatus	1.3.6.1.4.1.2272.1.220.1.2.5.1.6	9.0.3
rcLldpXMedLocMediaPolicyTagged	1.3.6.1.4.1.2272.1.220.1.2.5.1.7	9.0.3
rcPortNodeAliasClear	1.3.6.1.4.1.2272.1.4.10.1.1.140	9.1
rcMltNodeAliasClear	1.3.6.1.4.1.2272.1.17.10.1.50	9.1
rcNodeAlias	1.3.6.1.4.1.2272.1.234	9.1
rcNodeAliasMib	1.3.6.1.4.1.2272.1.234.1	9.1
rcNodeAliasObjects	1.3.6.1.4.1.2272.1.234.1.1	9.1
rcNodeAliasScalars	1.3.6.1.4.1.2272.1.234.1.1.1	9.1
rcNodeAliasClientsMaxNumberEntries	1.3.6.1.4.1.2272.1.234.1.1.1.1	9.1
rcNodeAliasClientsClearAll	1.3.6.1.4.1.2272.1.234.1.1.1.2	9.1
rcNodeAliasStatsTotalClientEntries	1.3.6.1.4.1.2272.1.234.1.1.1.3	9.1
rcNodeAliasStatsTotalActiveClientEntries	1.3.6.1.4.1.2272.1.234.1.1.1.4	9.1
rcNodeAliasStatsTotalProtocolInfoEntries	1.3.6.1.4.1.2272.1.234.1.1.1.5	9.1
rcNodeAliasGlobalEnable	1.3.6.1.4.1.2272.1.234.1.1.1.6	9.1
rcNodeAliasEnabledPortList	1.3.6.1.4.1.2272.1.234.1.1.1.7	9.1
rcNodeAliasClientTable	1.3.6.1.4.1.2272.1.234.1.1.2	9.1
rcNodeAliasClientEntry	1.3.6.1.4.1.2272.1.234.1.1.2.1	9.1
rcNodeAliasClientEntryMacAddress	1.3.6.1.4.1.2272.1.234.1.1.2.1.1	9.1
rcNodeAliasClientEntryIsid	1.3.6.1.4.1.2272.1.234.1.1.2.1.2	9.1
rcNodeAliasClientEntryVlan	1.3.6.1.4.1.2272.1.234.1.1.2.1.3	9.1
rcNodeAliasClientEntryInterfaceIndex	1.3.6.1.4.1.2272.1.234.1.1.2.1.4	9.1
rcNodeAliasClientEntryHostname	1.3.6.1.4.1.2272.1.234.1.1.2.1.5	9.1
rcNodeAliasClientEntryOSType	1.3.6.1.4.1.2272.1.234.1.1.2.1.6	9.1
rcNodeAliasClientEntryOSVersion	1.3.6.1.4.1.2272.1.234.1.1.2.1.7	9.1
rcNodeAliasClientEntryDeviceType	1.3.6.1.4.1.2272.1.234.1.1.2.1.8	9.1
rcNodeAliasClientEntryCapabilities	1.3.6.1.4.1.2272.1.234.1.1.2.1.9	9.1
rcNodeAliasClientEntryIsActive	1.3.6.1.4.1.2272.1.234.1.1.2.1.10	9.1

Table 55: Common (continued)

Object Name	Object OID	New in Release
rcNodeAliasClientEntryFirstLearnedTimer	1.3.6.1.4.1.2272.1.234.1.1.2.1.11	9.1
rcNodeAliasClientEntryLastLearnedTimer	1.3.6.1.4.1.2272.1.234.1.1.2.1.12	9.1
rcNodeAliasClientEntryReference	1.3.6.1.4.1.2272.1.234.1.1.2.1.13	9.1
rcNodeAliasClientEntryIpv4Addr	1.3.6.1.4.1.2272.1.234.1.1.2.1.14	9.1
rcNodeAliasClientEntryIpv6Addr	1.3.6.1.4.1.2272.1.234.1.1.2.1.15	9.1
rcNodeAliasClientEntryClear	1.3.6.1.4.1.2272.1.234.1.1.2.1.16	9.1
rcNodeAliasClientEntryIsidValue	1.3.6.1.4.1.2272.1.234.1.1.2.1.17	9.1
rcNodeAliasProtocolInfoTable	1.3.6.1.4.1.2272.1.234.1.1.3	9.1
rcNodeAliasProtocolInfoEntry	1.3.6.1.4.1.2272.1.234.1.1.3.1	9.1
rcNodeAliasProtocolInfoSourceMacAddress	1.3.6.1.4.1.2272.1.234.1.1.3.1.1	9.1
rcNodeAliasProtocolInfoIsid	1.3.6.1.4.1.2272.1.234.1.1.3.1.2	9.1
rcNodeAliasProtocolInfoVlan	1.3.6.1.4.1.2272.1.234.1.1.3.1.3	9.1
rcNodeAliasProtocolInfoInterfaceIndex	1.3.6.1.4.1.2272.1.234.1.1.3.1.4	9.1
rcNodeAliasProtocolInfoProtocolType	1.3.6.1.4.1.2272.1.234.1.1.3.1.5	9.1
rcNodeAliasProtocolInfoValue	1.3.6.1.4.1.2272.1.234.1.1.3.1.6	9.1
rcNodeAliasProtocolInfoLastLearnedTimer	1.3.6.1.4.1.2272.1.234.1.1.3.1.7	9.1
rcNodeAliasProtocolInfoIsidValue	1.3.6.1.4.1.2272.1.234.1.1.3.1.8	9.1
rcNodeAliasDhcpFingerprintTable	1.3.6.1.4.1.2272.1.234.1.1.4	9.1
rcNodeAliasDhcpFingerprintEntry	1.3.6.1.4.1.2272.1.234.1.1.4.1	9.1
rcNodeAliasDhcpFingerprintSourceMacAddress	1.3.6.1.4.1.2272.1.234.1.1.4.1.1	9.1
rcNodeAliasDhcpFingerprintIsid	1.3.6.1.4.1.2272.1.234.1.1.4.1.2	9.1
rcNodeAliasDhcpFingerprintVlan	1.3.6.1.4.1.2272.1.234.1.1.4.1.3	9.1
rcNodeAliasDhcpFingerprintInterfaceIndex	1.3.6.1.4.1.2272.1.234.1.1.4.1.4	9.1
rcNodeAliasDhcpFingerprintIpv4Addr	1.3.6.1.4.1.2272.1.234.1.1.4.1.5	9.1
rcNodeAliasDhcpFingerprintOption12	1.3.6.1.4.1.2272.1.234.1.1.4.1.6	9.1
rcNodeAliasDhcpFingerprintOption55	1.3.6.1.4.1.2272.1.234.1.1.4.1.7	9.1

Table 55: Common (continued)

Object Name	Object OID	New in Release
rcNodeAliasDhcpFingerprintOption60	1.3.6.1.4.1.2272.1.234.1.1.4.1.8	9.1
rcNodeAliasDhcpFingerprintIsidValue	1.3.6.1.4.1.2272.1.234.1.1.4.1.9	9.1
rcRadiusServHostSecureOcsp	1.3.6.1.4.1.2272.1.29.5.1.35	9.1
rcIpRedistributeInterVrfAutoFilterTag	1.3.6.1.4.1.2272.1.8.100.22.1.16	9.1
rcIsisGlobalDesignatedBNHostName	1.3.6.1.4.1.2272.1.63.1.35	9.1
rcIsisGlobalDesignatedBNHomeSystemId	1.3.6.1.4.1.2272.1.63.1.36	9.1
rcIsisGlobalDesignatedBNRemoteSystemId	1.3.6.1.4.1.2272.1.63.1.37	9.1
rcIsisMultiAreaL3RedistributeDeleteTags	1.3.6.1.4.1.2272.1.63.29.2.5.1.7	9.1
rcIpAnycastGwInterfaceTable	1.3.6.1.4.1.2272.1.8.34	9.1
rcIpAnycastGwInterfaceEntry	1.3.6.1.4.1.2272.1.8.34.1	9.1
rcIpAnycastGwInterfaceL2vsnIsid	1.3.6.1.4.1.2272.1.8.34.1.1	9.1
rcIpAnycastGwInterfaceGwAddrType	1.3.6.1.4.1.2272.1.8.34.1.2	9.1
rcIpAnycastGwInterfaceGwAddr	1.3.6.1.4.1.2272.1.8.34.1.3	9.1
rcIpAnycastGwInterfacePrefixLen	1.3.6.1.4.1.2272.1.8.34.1.4	9.1
rcIpAnycastGwInterfaceVrId	1.3.6.1.4.1.2272.1.8.34.1.5	9.1
rcIpAnycastGwInterfaceGwMac	1.3.6.1.4.1.2272.1.8.34.1.6	9.1
rcIpAnycastGwInterfaceVrfId	1.3.6.1.4.1.2272.1.8.34.1.7	9.1
rcIpAnycastGwInterfaceVlanId	1.3.6.1.4.1.2272.1.8.34.1.8	9.1
rcIpAnycastGwInterfaceOneIp	1.3.6.1.4.1.2272.1.8.34.1.9	9.1
rcIpAnycastGwInterfaceEnable	1.3.6.1.4.1.2272.1.8.34.1.10	9.1
rcIpAnycastGwInterfaceOperState	1.3.6.1.4.1.2272.1.8.34.1.11	9.1
rcIpAnycastGwInterfaceRowStatus	1.3.6.1.4.1.2272.1.8.34.1.12	9.1
rcIpAnycastGwIsidTable	1.3.6.1.4.1.2272.1.8.35	9.1
rcIpAnycastGwIsidEntry	1.3.6.1.4.1.2272.1.8.35.1	9.1
rcIpAnycastGwIsidL2vsnIsid	1.3.6.1.4.1.2272.1.8.35.1.1	9.1
rcIpAnycastGwIsidAdvSysId	1.3.6.1.4.1.2272.1.8.35.1.2	9.1
rcIpAnycastGwIsidGwAddrType	1.3.6.1.4.1.2272.1.8.35.1.3	9.1
rcIpAnycastGwIsidGwAddr	1.3.6.1.4.1.2272.1.8.35.1.4	9.1
rcIpAnycastGwIsidL3vsnIsid	1.3.6.1.4.1.2272.1.8.35.1.5	9.1

Table 55: Common (continued)

Object Name	Object OID	New in Release
rcIpAnycastGwIsidGwMac	1.3.6.1.4.1.2272.1.8.35.1.6	9.1
rcIpAnycastGwIsidPathCost	1.3.6.1.4.1.2272.1.8.35.1.7	9.1
rcIpAnycastGwIsidAddMetric	1.3.6.1.4.1.2272.1.8.35.1.8	9.1
rcIpAnycastGwIsidNextHopBmac	1.3.6.1.4.1.2272.1.8.35.1.9	9.1
rcIpAnycastGwIsidAdvRtrHostName	1.3.6.1.4.1.2272.1.8.35.1.10	9.1
rcIpAnycastGwIsidIsGwNode	1.3.6.1.4.1.2272.1.8.35.1.11	9.1
cabletron	1.3.6.1.4.1.52	9.1
mibs	1.3.6.1.4.1.52.4	9.1
ctron	1.3.6.1.4.1.52.4.1	9.1
ctNetwork	1.3.6.1.4.1.52.4.1.3	9.1
ctAliasMib	1.3.6.1.4.1.52.4.1.3.7	9.1
cabletronAliasMib	1.3.6.1.4.1.52.4.1.3.7.1	9.1
ctAlias	1.3.6.1.4.1.52.4.1.3.7.1.1	9.1
ctAliasTable	1.3.6.1.4.1.52.4.1.3.7.1.1.1	9.1
ctAliasEntry	1.3.6.1.4.1.52.4.1.3.7.1.1.1.1	9.1
ctAliasTimeFilter	1.3.6.1.4.1.52.4.1.3.7.1.1.1.1.1	9.1
ctAliasReference	1.3.6.1.4.1.52.4.1.3.7.1.1.1.1.2	9.1
ctAliasInterface	1.3.6.1.4.1.52.4.1.3.7.1.1.1.1.3	9.1
ctAliasMacAddress	1.3.6.1.4.1.52.4.1.3.7.1.1.1.1.4	9.1
ctAliasVlanID	1.3.6.1.4.1.52.4.1.3.7.1.1.1.1.5	9.1
ctAliasProtocol	1.3.6.1.4.1.52.4.1.3.7.1.1.1.1.6	9.1
ctAliasAddress	1.3.6.1.4.1.52.4.1.3.7.1.1.1.1.7	9.1
ctAliasIsActive	1.3.6.1.4.1.52.4.1.3.7.1.1.1.1.8	9.1
ctAliasAddressText	1.3.6.1.4.1.52.4.1.3.7.1.1.1.1.9	9.1
ctAliasMacAddressTable	1.3.6.1.4.1.52.4.1.3.7.1.1.5	9.1
ctAliasMacAddressEntry	1.3.6.1.4.1.52.4.1.3.7.1.1.5.1	9.1
ctAliasMacAddressInterface	1.3.6.1.4.1.52.4.1.3.7.1.1.5.1.1	9.1
ctAliasMacAddressVlanID	1.3.6.1.4.1.52.4.1.3.7.1.1.5.1.2	9.1
ctAliasMacAddressIsActive	1.3.6.1.4.1.52.4.1.3.7.1.1.5.1.3	9.1
ctAliasMacAddressAddressText	1.3.6.1.4.1.52.4.1.3.7.1.1.5.1.4	9.1
ctAliasMacAddressTime	1.3.6.1.4.1.52.4.1.3.7.1.1.5.1.5	9.1
ctAliasProtocolAddressTable	1.3.6.1.4.1.52.4.1.3.7.1.1.6	9.1
ctAliasProtocolAddressEntry	1.3.6.1.4.1.52.4.1.3.7.1.1.6.1	9.1

Table 55: Common (continued)

Object Name	Object OID	New in Release
ctAliasProtocolAddressInterface	1.3.6.1.4.1.52.4.1.3.7.1.1.6.1.1	9.1
ctAliasProtocolAddressVlanID	1.3.6.1.4.1.52.4.1.3.7.1.1.6.1.2	9.1
ctAliasProtocolAddressIsActive	1.3.6.1.4.1.52.4.1.3.7.1.1.6.1.3	9.1
ctAliasProtocolAddressAddressText	1.3.6.1.4.1.52.4.1.3.7.1.1.6.1.4	9.1
ctAliasProtocolAddressTime	1.3.6.1.4.1.52.4.1.3.7.1.1.6.1.5	9.1
ctAliasEntryClearAll	1.3.6.1.4.1.52.4.1.3.7.1.1.7	9.1
rcPortNodeAliasEnable	1.3.6.1.4.1.2272.1.4.10.1.1.139	9.1
rcVrfSdwanLocalBreakout	1.3.6.1.4.1.2272.1.203.1.1.1.2.1.15	9.1
bspePethPsePortDetectType	1.3.6.1.4.1.45.5.8.1.1.1.17	9.2
rcnIsisPlsbInterAreaDuplicatSysidTrap	1.3.6.1.4.1.2272.1.21.0.367	9.2
rcnIsisPlsbInterAreaDuplicateNicknameTrap	1.3.6.1.4.1.2272.1.21.0.368	9.2
rcIpv6RouterAdvertRdnssSuppress	1.3.6.1.4.1.2272.1.62.1.1.5.1.15	9.2
rcIpv6RouterAdvertDnsslSuppress	1.3.6.1.4.1.2272.1.62.1.1.5.1.16	9.2
rcIpv6RouterAdvertRdnssTable	1.3.6.1.4.1.2272.1.62.1.1.25	9.2
rcIpv6RouterAdvertRdnssEntry	1.3.6.1.4.1.2272.1.62.1.1.25.1	9.2
rcIpv6RouterAdvertRdnssIfIndex	1.3.6.1.4.1.2272.1.62.1.1.25.1.1	9.2
rcIpv6RouterAdvertRdnssSequence	1.3.6.1.4.1.2272.1.62.1.1.25.1.2	9.2
rcIpv6RouterAdvertRdnssLifetime	1.3.6.1.4.1.2272.1.62.1.1.25.1.3	9.2
rcIpv6RouterAdvertRdnssServer	1.3.6.1.4.1.2272.1.62.1.1.25.1.4	9.2
rcIpv6RouterAdvertRdnssRowStatus	1.3.6.1.4.1.2272.1.62.1.1.25.1.5	9.2
rcIpv6RouterAdvertDnsslTable	1.3.6.1.4.1.2272.1.62.1.1.26	9.2
rcIpv6RouterAdvertDnsslEntry	1.3.6.1.4.1.2272.1.62.1.1.26.1	9.2
rcIpv6RouterAdvertDnsslIfIndex	1.3.6.1.4.1.2272.1.62.1.1.26.1.1	9.2
rcIpv6RouterAdvertDnsslSequence	1.3.6.1.4.1.2272.1.62.1.1.26.1.2	9.2
rcIpv6RouterAdvertDnsslLifetime	1.3.6.1.4.1.2272.1.62.1.1.26.1.3	9.2
rcIpv6RouterAdvertDnsslDomain	1.3.6.1.4.1.2272.1.62.1.1.26.1.4	9.2
rcIpv6RouterAdvertDnsslRowStatus	1.3.6.1.4.1.2272.1.62.1.1.26.1.5	9.2
rcIsisHomeHostName	1.3.6.1.4.1.2272.1.63.9.50	9.2
rcIsisHomeChassisMac	1.3.6.1.4.1.2272.1.63.9.51	9.2
rcIsisHomeSysId	1.3.6.1.4.1.2272.1.63.9.52	9.2

Table 55: Common (continued)

Object Name	Object OID	New in Release
rcIsisRemoteSysId	1.3.6.1.4.1.2272.1.63.9.53	9.2
rcIsisDuplicateSysId	1.3.6.1.4.1.2272.1.63.9.54	9.2
rcIsisDuplicateNickname	1.3.6.1.4.1.2272.1.63.9.55	9.2
rcVossSystemMaxNormalizedTemperature	1.3.6.1.4.1.2272.1.101.1.1.1.9	9.2
rcVossSystemWarningThreshold	1.3.6.1.4.1.2272.1.101.1.1.1.10	9.2
rcVossSystemCriticalThreshold	1.3.6.1.4.1.2272.1.101.1.1.1.11	9.2
rcNlsServiceProbeTable	1.3.6.1.4.1.2272.1.223.24	9.2
rcNlsServiceProbeEntry	1.3.6.1.4.1.2272.1.223.24.1	9.2
rcNlsServiceProbeInstanceId	1.3.6.1.4.1.2272.1.223.24.1.1	9.2
rcNlsServiceProbeRowStatus	1.3.6.1.4.1.2272.1.223.24.1.2	9.2
rcNlsServiceProbeVlanId	1.3.6.1.4.1.2272.1.223.24.1.3	9.2
rcNlsServiceProbeIsid	1.3.6.1.4.1.2272.1.223.24.1.4	9.2
rcNlsServiceProbeState	1.3.6.1.4.1.2272.1.223.24.1.5	9.2
rcNlsServiceProbeMacAddr	1.3.6.1.4.1.2272.1.223.24.1.6	9.2
rcNlsServiceProbeIPOrigin	1.3.6.1.4.1.2272.1.223.24.1.7	9.2
rcNlsServiceProbeIPv4Address	1.3.6.1.4.1.2272.1.223.24.1.8	9.2
rcNlsServiceProbeIPv4Mask	1.3.6.1.4.1.2272.1.223.24.1.9	9.2
rcNlsServiceProbeIPv4DefaultGw	1.3.6.1.4.1.2272.1.223.24.1.10	9.2
rcNlsServiceProbeIPv4DefaultGwState	1.3.6.1.4.1.2272.1.223.24.1.11	9.2
rcNlsServiceProbeIPv4PingAddress	1.3.6.1.4.1.2272.1.223.24.1.12	9.2
rcNlsServiceProbeIPv4PingResult	1.3.6.1.4.1.2272.1.223.24.1.13	9.2
rcAutoSenseIsisStpMultiHomingOverwrite	1.3.6.1.4.1.2272.1.231.1.1.1.33	9.2

Table 56: 5320 Series

Object Name	Object OID	New in Release
rcDiagVctTable	1.3.6.1.4.1.2272.1.23.4	8.10
rcDiagVctEntry	1.3.6.1.4.1.2272.1.23.4.1	8.10
rcDiagVctIfIndex	1.3.6.1.4.1.2272.1.23.4.1.1	8.10
rcDiagVctNormalCableLength	1.3.6.1.4.1.2272.1.23.4.1.2	8.10
rcDiagVctCableStatus	1.3.6.1.4.1.2272.1.23.4.1.4	8.10
rcDiagVctPair1Status	1.3.6.1.4.1.2272.1.23.4.1.5	8.10

Table 56: 5320 Series (continued)

Object Name	Object OID	New in Release
rcDiagVctPair1ErrLength	1.3.6.1.4.1.2272.1.23.4.1.6	8.10
rcDiagVctPair2Status	1.3.6.1.4.1.2272.1.23.4.1.7	8.10
rcDiagVctPair2ErrLength	1.3.6.1.4.1.2272.1.23.4.1.8	8.10
rcDiagVctPair3Status	1.3.6.1.4.1.2272.1.23.4.1.9	8.10
rcDiagVctPair3ErrLength	1.3.6.1.4.1.2272.1.23.4.1.10	8.10
rcDiagVctPair4Status	1.3.6.1.4.1.2272.1.23.4.1.11	8.10
rcDiagVctPair4ErrLength	1.3.6.1.4.1.2272.1.23.4.1.12	8.10
rcDiagVctStartTest	1.3.6.1.4.1.2272.1.23.4.1.13	8.10
rcDiagVctTestDone	1.3.6.1.4.1.2272.1.23.4.1.14	8.10
rcDiagVctCableLength	1.3.6.1.4.1.2272.1.23.4.1.16	8.10
rcIsisPlsbNickNameOrigin	1.3.6.1.4.1.2272.1.63.4.1.19	8.10
rcIsisPlsbNickNameServerSysId	1.3.6.1.4.1.2272.1.63.4.1.20	8.10
rcIsisPlsbNickNameServerHostName	1.3.6.1.4.1.2272.1.63.4.1.21	8.10
rcIsisLogicalInterfaceIsisMtu	1.3.6.1.4.1.2272.1.63.26.1.33	8.10
rcLldpXMedLocMediaPolicyExtendedTable	1.3.6.1.4.1.2272.1.220.1.2.4	8.10
rcLldpXMedLocMediaPolicyExtendedEntry	1.3.6.1.4.1.2272.1.220.1.2.4.1	8.10
rcLldpXMedLocMediaPolicyExtendedOrigin	1.3.6.1.4.1.2272.1.220.1.2.4.1.1	8.10

Table 57: 5420 Series

Object Name	Object OID	New in Release
rcChasPowerSupplyDetailVoltageIn	1.3.6.1.4.1.2272.1.4.8.2.1.16	9.0.2
rcChasPowerSupplyDetailVoltageOut	1.3.6.1.4.1.2272.1.4.8.2.1.17	9.0.2
rcChasPowerSupplyDetailCurrentIn	1.3.6.1.4.1.2272.1.4.8.2.1.18	9.0.2
rcChasPowerSupplyDetailCurrentOut	1.3.6.1.4.1.2272.1.4.8.2.1.19	9.0.2
rcChasPowerSupplyDetailPowerIn	1.3.6.1.4.1.2272.1.4.8.2.1.20	9.0.2

Table 57: 5420 Series (continued)

Object Name	Object OID	New in Release
rcChasPowerSupplyDetailPowerOut	1.3.6.1.4.1.2272.1.4.8.2.1.21	9.0.2
rcAutoSenseSdWanVrfName	1.3.6.1.4.1.2272.1.231.1.1.1.32	9.0.3

Table 58: 5520 Series

Object Name	Object OID	New in Release
rcChasPowerSupplyDetailVoltageIn	1.3.6.1.4.1.2272.1.4.8.2.1.16	9.0.2
rcChasPowerSupplyDetailVoltageOut	1.3.6.1.4.1.2272.1.4.8.2.1.17	9.0.2
rcChasPowerSupplyDetailCurrentIn	1.3.6.1.4.1.2272.1.4.8.2.1.18	9.0.2
rcChasPowerSupplyDetailCurrentOut	1.3.6.1.4.1.2272.1.4.8.2.1.19	9.0.2
rcChasPowerSupplyDetailPowerIn	1.3.6.1.4.1.2272.1.4.8.2.1.20	9.0.2
rcChasPowerSupplyDetailPowerOut	1.3.6.1.4.1.2272.1.4.8.2.1.21	9.0.2
rcAutoSenseSdWanArea	1.3.6.1.4.1.2272.1.231.1.1.1.31	9.0.3
rcAutoSenseSdWanInterfaceTable	1.3.6.1.4.1.2272.1.231.1.1.2	9.0.3
rcAutoSenseSdWanInterfaceIp	1.3.6.1.4.1.2272.1.231.1.1.2.1.1	9.0.3
rcAutoSenseSdWanInterfaceRowStatus	1.3.6.1.4.1.2272.1.231.1.1.2.1.2	9.0.3
rcAutoSenseSdWanInterfaceArea	1.3.6.1.4.1.2272.1.231.1.1.2.1.3	9.0.3
rcAutoSenseSdWanVrfName	1.3.6.1.4.1.2272.1.231.1.1.1.32	9.0.3

Table 59: 5720 Series

Object Name	Object OID	New in Release
rcChasPowerSupplyDetailVoltageIn	1.3.6.1.4.1.2272.1.4.8.2.1.16	9.0.2
rcChasPowerSupplyDetailVoltageOut	1.3.6.1.4.1.2272.1.4.8.2.1.17	9.0.2
rcChasPowerSupplyDetailCurrentIn	1.3.6.1.4.1.2272.1.4.8.2.1.18	9.0.2
rcChasPowerSupplyDetailCurrentOut	1.3.6.1.4.1.2272.1.4.8.2.1.19	9.0.2

Table 59: 5720 Series (continued)

Object Name	Object OID	New in Release
rcChasPowerSupplyDetailPowerIn	1.3.6.1.4.1.2272.1.4.8.2.1.20	9.0.2
rcChasPowerSupplyDetailPowerOut	1.3.6.1.4.1.2272.1.4.8.2.1.21	9.0.2
rcAutoSenseSdWanArea	1.3.6.1.4.1.2272.1.231.1.1.1.31	9.0.3
rcAutoSenseSdWanInterfaceTable	1.3.6.1.4.1.2272.1.231.1.1.2	9.0.3
rcAutoSenseSdWanInterfaceIp	1.3.6.1.4.1.2272.1.231.1.1.2.1.1	9.0.3
rcAutoSenseSdWanInterfaceRowStatus	1.3.6.1.4.1.2272.1.231.1.1.2.1.2	9.0.3
rcAutoSenseSdWanInterfaceArea	1.3.6.1.4.1.2272.1.231.1.1.2.1.3	9.0.3
rcAutoSenseSdWanVrfName	1.3.6.1.4.1.2272.1.231.1.1.1.32	9.0.3

Table 60: 7520 Series

Object Name	Object OID	New in Release
rcChasPowerSupplyDetailVoltageIn	1.3.6.1.4.1.2272.1.4.8.2.1.16	9.0.2
rcChasPowerSupplyDetailVoltageOut	1.3.6.1.4.1.2272.1.4.8.2.1.17	9.0.2
rcChasPowerSupplyDetailCurrentIn	1.3.6.1.4.1.2272.1.4.8.2.1.18	9.0.2
rcChasPowerSupplyDetailCurrentOut	1.3.6.1.4.1.2272.1.4.8.2.1.19	9.0.2
rcChasPowerSupplyDetailPowerIn	1.3.6.1.4.1.2272.1.4.8.2.1.20	9.0.2
rcChasPowerSupplyDetailPowerOut	1.3.6.1.4.1.2272.1.4.8.2.1.21	9.0.2
rcAutoSenseSdWanArea	1.3.6.1.4.1.2272.1.231.1.1.1.31	9.0.3
rcAutoSenseSdWanInterfaceTable	1.3.6.1.4.1.2272.1.231.1.1.2	9.0.3
rcAutoSenseSdWanInterfaceIp	1.3.6.1.4.1.2272.1.231.1.1.2.1.1	9.0.3
rcAutoSenseSdWanInterfaceRowStatus	1.3.6.1.4.1.2272.1.231.1.1.2.1.2	9.0.3

Table 60: 7520 Series (continued)

Object Name	Object OID	New in Release
rcAutoSenseSdWanInterfaceArea	1.3.6.1.4.1.2272.1.231.1.1.2.1.3	9.0.3
rcAutoSenseSdWanVrfName	1.3.6.1.4.1.2272.1.231.1.1.1.32	9.0.3

Table 61: 7720 Series

Object Name	Object OID	New in Release
rcChasPowerSupplyDetailVoltageIn	1.3.6.1.4.1.2272.1.4.8.2.1.16	9.0.2
rcChasPowerSupplyDetailVoltageOut	1.3.6.1.4.1.2272.1.4.8.2.1.17	9.0.2
rcChasPowerSupplyDetailCurrentIn	1.3.6.1.4.1.2272.1.4.8.2.1.18	9.0.2
rcChasPowerSupplyDetailCurrentOut	1.3.6.1.4.1.2272.1.4.8.2.1.19	9.0.2
rcChasPowerSupplyDetailPowerIn	1.3.6.1.4.1.2272.1.4.8.2.1.20	9.0.2
rcChasPowerSupplyDetailPowerOut	1.3.6.1.4.1.2272.1.4.8.2.1.21	9.0.2
rcAutoSenseSdWanArea	1.3.6.1.4.1.2272.1.231.1.1.1.31	9.0.3
rcAutoSenseSdWanInterfaceTable	1.3.6.1.4.1.2272.1.231.1.1.2	9.0.3
rcAutoSenseSdWanInterfaceIp	1.3.6.1.4.1.2272.1.231.1.1.2.1.1	9.0.3
rcAutoSenseSdWanInterfaceRowStatus	1.3.6.1.4.1.2272.1.231.1.1.2.1.2	9.0.3
rcAutoSenseSdWanInterfaceArea	1.3.6.1.4.1.2272.1.231.1.1.2.1.3	9.0.3
rcAutoSenseSdWanVrfName	1.3.6.1.4.1.2272.1.231.1.1.1.32	9.0.3

Obsolete MIBs

Table 62: Common

Object Name	Object OID	Obsolete in Release
rcIpBgpTmpEstablishedNotification	1.3.6.1.4.1.2272.1.8.101.17.0.1	8.10.1
rcIpBgpTmpBackwardTransNotification	1.3.6.1.4.1.2272.1.8.101.17.0.2	8.10.1