Release Notes for VSP Operating System Software

Release 5.3
NN47227-401
Issue 13.03
April 2017

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

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

Licence types

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

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose

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

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

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

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

Chapter 2: New in this document

The following sections detail what is new in *Release Notes for VSP Operating System Software*, NN47227-401.

Hardware

VOSS 5.3 introduces the following new hardware:

VSP 8404C

The VSP 8404C is a flexible, compact form-factor Ethernet switch that not only provides all of the features of other VSP 8400 series switches, but also enables the use of 100 Gbps Ethernet Switch Modules (ESM).

❗ **Important:**

VOSS 5.3 software is supported only on the VSP 8404C hardware platform. It is not supported on other hardware platforms.

8402CQ ESM

The 8402CQ Ethernet Switch Module (ESM) is a 2 port 100 Gbps QSFP28 ESM. It is for use only with the VSP 8404C hardware platform.

For more information on the VSP 8404C or the 8402CQ ESM, see *Installing the Avaya Virtual Services Platform 8000 Series*.

100 Gbps QSFP28 transceivers and cables

Table 1: New 100 Gbps QSFP28 transceivers

Transceiver	Reach	Part number
100GBASE-SR4	70 m with OM3 multimode fiber cable 100 m with OM4 multimode fiber cable	AA1405005–E6

Table 2: New 100–gigabit QSFP28 cables

Cable type	Cable Length	Part number
QSFP28 to QSFP28 100-gigabit (passive)		
Passive copper DAC	1 meter	AA1405029–E6
Passive copper DAC	3 meter	AA1405031–E6

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

Firmware upgrade of 8424XT and 8418XTQ ESMs on VSP 8404C

On a VSP 8404C switch running the 5.3.0.0 software image, the PHY firmware version of the tri-speed 100M/1G/10G copper ports is automatically upgraded to version 1.9.1 either during boot up or when you insert the 8424XT or the 8418XTQ ESM. The software checks the existing firmware version associated with these ports and automatically upgrades them. It also reinitializes the ESM for the new firmware version to take effect. The firmware upgrade process takes about 40 seconds and the reinitialization of the ESM takes about 50 seconds.

The switch displays information about the version check and upgrade in its log messages. A sample log message is as follows:

```
IO1 [12/06/16 10:59:28.290:UTC] 0x001205f7 00000000 GlobalRouter COP-SW
INFO Slot 2 ESM PHY:84848 has firmware rev:1. 8. 0. Min Required: 1. 9.
1. Performing Update

IO1 [12/06/16 11:00:05.672:UTC] 0x001205f6 00000000 GlobalRouter COP-SW
INFO Slot 2 PHY firmware updated. The ESM will be reinitialized.

CP1 [12/06/16 11:00:52.562:UTC] 0x00010750 00000000 GlobalRouter HW INFO
Module 8418XTQ in slot 2 is ready for configuration download
```

⚠ **Caution:**

Do not remove an ESM during boot up or after a hot insertion until you see the log message indicating that the reinitialization is complete.

An ESM with the firmware version upgraded to version 1.9.1 can be safely used on VSP 8404 platforms running older software releases.

Features

VOSS 5.3 supports all the features available in VOSS 5.1.1 and in addition, supports the following features.

Bridge Protocol Data Unit (BPDU) Guard

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

For more information, see the following sections:

- BPDU Guard on page 13
- Configuring BPDU Guard using the CLI on page 14
- Configuring BPDU Guard using the EDM on page 15
- Troubleshooting BPDU Guard on page 16

CLI command updates to include additional parameter

The following CLI commands are updated to include the mgmtEthernet mgmt parameter:

- **`show ipv6 nd interface`**
- **`show ipv6 dcache`**

For more information, see the following tasks:

- Viewing global IPv6 information on page 20
- Viewing cached destination information on page 25

Entity MIB — Physical Table

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

For more information, see the following sections:

- Entity MIB – Physical Table on page 27
- Viewing physical entities on page 27

IEEE 802.3X Pause frame transmit

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

For more information, see the following sections:

- IEEE 802.3X Pause frame transmit on page 30

- Configuring IEEE 802.3X Pause frame transmit using the CLI on page 32
- Configuring IEEE 802.3X Pause frame transmit using the EDM on page 34

For information on viewing statistics to manage network performance, see Viewing port interface statistics on page 35.

Link Layer Discovery Protocol (LLDP)

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

For more information, see the following sections:

- Link Layer Discovery Protocol (802.1AB) fundamentals on page 37
- Link Layer Discovery Protocol configuration using CLI on page 40
- Link Layer Discovery Protocol configuration using EDM on page 50

SMTP for email notification

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

For more information, see the following sections:

- Email notification on page 58
- Configuring email notification using the CLI on page 60
- Configuring email notification using the EDM on page 64

Support for 100 Gbps Ethernet

100 GbE port considerations on page 66 is added to the document to address Clause 91 Forward Error Correction and auto-negotiation.

Port-based shaping:

The shaping rate is updated to reflect support for 100 Gbps ports. For more information, see Configuring the port-based shaper on page 67.

OSPF default metric:

The OSPF default metric is updated to include support for 100 Gbps. For more information, see the following tasks:

- Configuring OSPF globally using the CLI on page 67
- Configuring OSPF globally using the EDM on page 69
- Viewing the OSPF default cost information on page 72
- Configuring global default metrics on page 74
- Configuring OSPF default metrics on page 73
- Configuring OSPFv3 globally on page 75
- Viewing OSPFv3 default cost information on page 76

Support for 100 Gbps QSFP28 transceivers

Resetting a QSFP+ or QSFP28 transceiver:

Resetting a QSFP+ or QSFP28 transceiver on page 77 is retitled to include QSFP28 (100 Gbps) transceivers. In previous document issues, the content was specific to QSFP+ (40 Gbps) transceivers.

Digital Diagnostic Monitoring:

Digital Diagnostic Interface (DDI) information is updated to include 100 Gbps transceivers. For more information, see Digital Diagnostic Monitoring on page 78.

VOSS feature differences

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

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

Feature	VSP 4000 Series	VSP 7200 Series	VSP 8000 Series
Channelization of 40 Gbps ports	Not applicable	Supported	Supported
CMAC — CFM	Supported	Not supported	Not supported
vms install script	Supported	Not supported	Not supported
FDB protected by port	Supported	Not supported	Not supported
Multicast Route Statistics for IPv4 and IPv6	Not supported	Supported	Supported
NLB unicast	Not supported	Supported	Supported
PoE/PoE+ Allocation Using LLDP	Supported on VSP 4850GTS-PWR+ and VSP 4450GTX-HT-PWR +	Not supported	Not supported
Port licensing	Not supported	Applicable to Port licensed VSP 7254XSQ fiber switch and VSP 7254XTQ copper switch	Not supported
QoS	Supported	Supported with exceptions: • Classification does not have routed packet classification	Supported with exceptions: • Classification does not have routed packet classification

Table continues…

Feature	VSP 4000 Series	VSP 7200 Series	VSP 8000 Series
		• No ingress policer-Uses ingress port rate limiting instead	• No ingress policer-Uses ingress port rate limiting instead
Software licensing (Premier)	Supports the Avaya Data Licensing Portal and the Product Licensing & Delivery System (PLDS)	Supports Product Licensing & Delivery System (PLDS) only	Supports Product Licensing & Delivery System (PLDS) only
Use of Open Networking Adapter for Fabric Extend	Required	Not required	Not required

Chapter 3: Features in VOSS 5.3

VOSS 5.3 supports all the features available in VOSS 5.1.1 and in addition, supports new features. See the following sections for information about the new features.

Bridge Protocol Data Unit (BPDU) Guard

BPDU Guard

The switch supports Bridge Protocol Data Unit (BPDU) Guard for STGs, RSTP, and MSTP.

Overview

Spanning Tree eliminates loops in a network. A bridge that participates in spanning tree uses BPDUs to exchange information with other bridges. The bridges select a single bridge as the root bridge based on the BPDU information exchange. The bridge with the lowest priority becomes the root bridge. If all bridges share the same priority, the bridge with the lowest bridge ID becomes the root bridge. This process is the root selection process.

After you add a new bridge to the network, or remove an existing bridge, the bridges repeat the root selection process, and then select a new root bridge.

To ensure the correct operation of Spanning Tree in the network, BPDU Guard protects the stability of the Root Bridge by dropping stray, unexpected, or unwanted BPDU packets entering a port, and immediately shutting down those ports for a specified time period. BPDU Guard is normally enabled on access ports connecting to end user devices such as servers that are not expected to operate Spanning Tree.

Use BPDU Guard to achieve the following results:

- Block the root selection process after an edge device, such as a laptop that uses Linux with STP enabled, is added to the network. Blocking the root selection process prevents unknown devices from influencing the spanning tree topology.
- Block BPDU flooding of the switch from an unknown device.

Operation

You can enable or disable BPDU Guard on an individual port basis, regardless of the spanning tree state. Each port uses a timer to determine port-state recovery.

After you enable BPDU Guard on a port and the port receives a BPDU, the following actions occur:

1. The guard disables the port.
2. The switch generates an SNMP trap and alarm, and the following log message:

   ```
   BPDU Guard - Port <slot/port> is being shutdown by BPDU Guard,
   timeout <time_seconds>
   ```

3. The port timer begins.
4. The port remains in the disabled state until the timer expires.

If you disable BPDU Guard before the timer expires, the timer stops and the port remains in the disabled state. You must manually enable the port.

BPDU Guard is enabled at the interface level. You can configure the BPDU Guard timer for each port, for 10 to 65535 seconds. If you set the port timer to zero, it will not expire.

Configuring BPDU Guard

Configure BPDU Guard to block the root selection process or to prevent BPDU flooding from unknown devices.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Enable BPDU Guard for the port:

   ```
   spanning-tree bpduguard enable
   ```

3. **(Optional)** Configure the timer for port-state recovery:

   ```
   spanning-tree bpduguard timeout <0, 10-65535>
   ```

4. **(Optional)** Enable BPDU Guard on an additional port or group of ports:

   ```
   spanning-tree bpduguard port {slot/port[/sub-port][-slot/port[/
   subport]][,...]} enable
   ```

5. **(Optional)** Configure the timer for port-state recovery for an additional port or group of ports:

   ```
   spanning-tree bpduguard port {slot/port[/sub-port][-slot/port[/
   subport]][,...]} timeout <0-65535>
   ```

6. Verify the configuration:

   ```
   show spanning-tree bpduguard [GigabitEthernet {slot/port[/sub-port]
   [-slot/port[/subport]][,...]}] [{slot/port[/sub-port][-slot/port[/
   subport]][,...]}]
   ```

Example

Enable BPDU Guard on port 1/8, and specify a timer value of 200 seconds. Verify the configuration.

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#interface gigabitEthernet 1/8
Switch:1(config-if)#spanning-tree bpduguard enable
Switch:1(config-if)#spanning-tree bpduguard timeout 200
Switch:1(config-if)#show spanning-tree bpduguard 1/8

==============================================================
                                    Bpdu Guard
==============================================================
Port      PORT          PORT                 TIMER   BPDUGUARD
NUM MLTID ADMIN_STATE   OPER_STATE TIMEOUT   COUNT   ADMIN_STATE
------------------------------------------------------------------
1/8       Up             Up        200         0       Enabled
```

Variable definitions

Use the data in the following table to use the **spanning-tree bpduguard** commands.

Variable	Value
enable	Enables BPDU Guard on the port. The default is disabled.
port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).
timeout *<0, 10-65535>*	Specifies the value to use for port-state recovery. After a BPDU guard disables a port, the port remains in the disabled state until this timer expires. You can configure a value from 10 to 65535. The default is 120 seconds. If you configure the value to 0, the expiry is infinity.

Use the data in the following table to use the **show spanning-tree bpduguard** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

Configuring BPDU Guard

Configure BPDU Guard to block the root selection process or to prevent BPDU flooding from unknown devices.

About this task

To configure multiple ports simultaneously, select more than one port in the Device Physical View tab. The **BPDU Guard** tab appears as a table-based tab. For more information about how to use a table-based tab, see *Using CLI and EDM*.

Procedure

1. In the Device Physical View tab, select a port.
2. In the navigation pane, expand the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. Click the **Interface** tab.
5. Select **BpduGuardAdminEnabled** to enable BPDU Guard for the port.
6. **(Optional)** Type a value in **BpduGuardTimeout** to configure the timer for port-state recovery
7. Click **Apply**.

BPDU Guard field descriptions

Use the data in the following table to use the **Interface** tab for BPDU Guard.

Name	Description
BpduGuardAdminEnabled	Enables BPDU Guard on the port. The default is disabled.
BpduGuardTimeout	Specifies the value to use for port-state recovery. After a BPDU guard disables a port, the port remains in the disabled state until this timer expires. You can configure a value of 0 or from 10 to 6553500. The default is 12000 (1/100 seconds). For example, a value of 1000 equals 10 seconds. ✱ **Note:** If you configure the value to 0, you disable the timer, and the port timer does not expire.
BpduGuardTimerCount	Shows the time, starting at 0, since the port became disabled. When the BpduGuardTimerCount reaches the BpduGuardTimeout value, the port is enabled. Displays in 1/100 seconds.

Troubleshooting BPDU Guard

The following procedures provide information to troubleshoot issues with Bridge Protocol Data Unit (BPDU) Guard.

No packets received on the port

For BPDU Guard to work on a port, the port must receive BPDU packets. Perform the following procedure to troubleshoot cases when the port does not receive packets.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Show the BPDU Guard status for the port:

   ```
   show spanning-tree bpduguard {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

3. Use the following command to verify that the port receives packets:

   ```
   show interface gigabitEthernet statistics verbose {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

4. Verify that the remote port is sending packets:

   ```
   show spanning-tree {mstp|rstp} port role [{slot/port[/sub-port][-slot/port[/sub-port]][,...]}]
   ```

   ```
   show spanning-tree {mstp|rstp} port statistics [{slot/port[/sub-port][-slot/port[/sub-port]][,...]}]
   ```

Example

Port 1/8 receives packets. The remote port is disabled and does not send BPDU packets.

The following example shows that BPDU Guard is enabled for port 1/8. The BPDU Guard administrative state for the port is enabled but the timer counter is 0.

```
Switch:1>enable
Switch:1#show spanning-tree bpduguard 1/8
============================================================
                                   Bpdu Guard
============================================================
Port      PORT         PORT                TIMER    BPDUGUARD
NUM MLTID ADMIN_STATE  OPER_STATE TIMEOUT  COUNT   ADMIN_STATE
----------------------------------------------------------------
1/8        Up           Up         120      0       Enabled
Switch:1#show interface gigabitEthernet statistics verbose 1/8
==========================================================================================
=======
                                          Port Stats Interface Extended
==========================================================================================
=======
PORT_NUM IN_UNICST  OUT_UNICST IN_MULTICST  OUT_MULTICST IN_BRDCST  OUT_BRDCST   IN_LSM
OUT_LSM
------------------------------------------------------------------------------------------
-------
1/8    201          0          160062       60943        4          72
0         0
Switch:1#show spanning-tree mstp port role 1/8
================================================================================
                           CIST Port Roles and States
================================================================================
Port-Index  Port-Role    Port-State   PortSTPStatus  PortOperStatus
```

```
--------------------------------------------------------------------------------
1/8       Disabled     Forwarding   Disabled       Disabled
Switch:1#show spanning-tree mstp port statistics 1/8
================================================================================
                           MSTP Cist Port Statistics
================================================================================
Port Number                        : 1/8
Cist Port Fwd Transitions          : 0
Cist Port Rx MST BPDUs Count       : 0
Cist Port Rx RST BPDUs Count       : 0
Cist Port Rx Config BPDUs Count    : 0
Cist Port Rx TCN BPDUs Count       : 0
Cist Port Tx MST BPDUs Count       : 0
Cist Port Tx RST BPDUs Count       : 0
Cist Port Tx Config BPDUs Count    : 0
Cist Port Tx TCN BPDUs Count       : 0
Cist Port Invalid MSTP BPDUs Rx    : 0
Cist Port Invalid RST BPDUs Rx     : 0
Cist Port Invalid Config BPDUs Rx  : 0
Cist Port Invalid TCN BPDUs Rx     : 0
Cist Port Proto Migr Count         : 0
```

Variable definitions

Use the data in the following table to use the **`show spanning-tree bpduguard`** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

Use the data in the following table to use the **`show interface gigabitEthernet statistics verbose`** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

Use the data in the following table to use the **`show spanning-tree`** command.

Variable	Value
{mstp|rstp}	Specifies the spanning tree protocol.
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

SNMP trap not received

Perform the following procedure to troubleshoot issues in which an SNMP trap is not received.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Show the BPDU Guard status for the port:

   ```
   show spanning-tree bpduguard {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

3. Configure the correct SNMP target information:

   ```
   snmp-server host WORD<1-256> [port <1-65535>] v3 {noAuthNoPriv|authNoPriv|authPriv WORD<1-32> [inform [timeout <1-2147483647>] [retries <0-255>]] [filter WORD<1-32>]
   ```

Example

In the following example, BPDU guard is enabled on port 1/8, BPDU packets are received, port 1/8 is disabled, and the TimerCount is incrementing, but no SNMP trap is ever received.

```
Switch:1>enable
Switch:1#show spanning-tree bpduguard 1/8

================================================================================
                                   Bpdu Guard
================================================================================
Port           PORT        PORT                    TIMER BPDUGUARD
NUM      MLTID ADMIN_STATE OPER_STATE  TIMEOUT  COUNT ADMIN_STATE
--------------------------------------------------------------------------------
1/8            Down        Down        120      0     Disabled
```

Variable definitions

Use the data in the following table to use the **show spanning-tree** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

Use the data in the following table to use the **snmp-server host** command.

Variable	Value
filter *WORD<1-32>*	Specifies a filter profile name.
host *WORD<1-256>*	Specifies the IPv4 or IPv6 host address
inform [timeout *<1-2147483647>*]	Specifies the notify type. The optional timeout parameter configures the timeout value, which specifies the time to wait for a reply before resending

Table continues…

Variable	Value
	the inform message. Time is specified in centiseconds
noAuthNoPriv|authNoPriv|authPriv *WORD<1-32>*	Specifies the security level.
port *<1-65535>*	Specifies the port number that will be set as the destination port at the UDP level in the trap packet.
retries *<0-255>*	Specifies the number of packets to be sent if no reply is received.
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

CLI command updates to include additional parameter

The following CLI commands are updated to include the mgmtEthernet mgmt parameter:

- **`show ipv6 nd interface`**
- **`show ipv6 dcache`**

See the tasks in this section for more information.

Viewing global IPv6 information

Use the following procedure to view and manage general IPv6 information.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display IPv6 information for an interface:

   ```
   show ipv6 interface [gigabitethernet {slot/port[/sub-port] [-slot/
   port[/sub-port]] [,...]}] [loopback <1-256>][mgmtEthernet {slot/
   port[/sub-port][-slot/port[/sub-port]][,...]}][tunnel <1-2000>][vlan
   <1-4059>]
   ```

3. Display IPv6 tunnel information:

   ```
   show ipv6 interface tunnel
   ```

4. Display IPv6 address information for the specified slot and port:

   ```
   show ipv6 address interface gigabitethernet {slot/port[/sub-port] [-
   slot/port[/sub-port]] [,...]}
   ```

5. Display IPv6 address information for the specified IPv6 address:

```
show ipv6 address interface ip WORD<0-46>
```

6. Display IPv6 address information for the specified tunnel :

   ```
   show ipv6 address interface tunnel <1-2000>
   ```

7. Display IPv6 address information for the specified VLAN:

   ```
   show ipv6 address interface vlan <1-4059>
   ```

8. Display the current state of IPv6 forwarding:

   ```
   show ipv6 forwarding
   ```

9. Display information on the current state of IPv6 functionality:

   ```
   show ipv6 global
   ```

10. Display IPv6 Gigabit Ethernet (GbE) router advertisement information:

    ```
    show ipv6 nd interface gigabitethernet [{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]
    ```

11. Display IPv6 router advertisement information for the management port:

    ```
    show ipv6 nd interface mgmtEthernet mgmt
    ```

    Note:

    This step only applies to hardware with a dedicated, physical management interface.

12. Display IPv6 VLAN router advertisement information:

    ```
    show ipv6 nd interface vlan [<1-4059>]
    ```

13. Display detailed information in IPv6 router advertisements:

    ```
    show ipv6 nd-prefix detail
    ```

14. Display GbE interface information in IPv6 router advertisements:

    ```
    show ipv6 nd-prefix interface gigabitethernet [{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]
    ```

15. Display VLAN interface information in IPv6 router advertisements:

    ```
    show ipv6 nd-prefix interface vlan [<1-4059>]
    ```

16. Display VLAN information in IPv6 router advertisements:

    ```
    show ipv6 nd-prefix vlan <1-4059>
    ```

17. Display IPv6 neighbor entries with specific brouter port numbers:

    ```
    show ipv6 neighbor interface gigabitethernet {slot/port[/sub-port]}
    ```

18. Display IPv6 neighbor information for neighbors of the specified type:

    ```
    show ipv6 neighbor type <1-4>
    ```

19. Display IPv6 neighbor information:

show ipv6 neighbor [*WORD<0-46>*]

Example

```
Switch:1(config)#show ipv6 interface vlan

===========================================================================================================================
                                             Vlan Ipv6 Interface
===========================================================================================================================
IFINDX VLAN PHYSICAL          ADMIN   OPER  TYPE  MTU  HOP REACHABLE   RETRANSMIT  MCAST    IPSEC    RPC      RPCMODE
INDX        ADDRESS           STATE   STATE             LMT TIME        TIME        STATUS
---------------------------------------------------------------------------------------------------------------------------
2070   22   e4:5d:52:3c:65:02 disable down  ETHER 1500 64  30000       1000        disable  disable  disable  existonly

===========================================================================================================================
                               Vlan Ipv6 Address
===========================================================================================================================
IPV6 ADDRESS                            VLAN-ID      TYPE    ORIGIN    STATUS
---------------------------------------------------------------------------------------------------------------------------
fe80:0:0:0:e65d:52ff:fe3c:6502          V-22         UNICAST LINKLAYER INACCESSIBLE

1 out of 2 Total Num of Interface Entries displayed.
1 out of 2 Total Num of Address Entries displayed.
```

```
Switch:1#show ipv6 interface tunnel

======================================================================================================
Tunnel Ipv6 Interface
======================================================================================================
IF   Descr         VLAN PHYSICAL          ADMIN   OPER  TYPE  MTU  HOP REACHABLE RETRANSMIT  MCAST
INDX                    ADDRESS           STATE   STATE             LMT TIME      TIME       STATUS
------------------------------------------------------------------------------------------------------
6656 T-1           0    n/a               enable  up    P2P   1280 64  30000     1000      disable
6657 T-2           0    n/a               enable  up    P2P   1280 64  30000     1000      disable

=======================================================================================================
                              Tunnel Ipv6 Address
=======================================================================================================
IPV6 ADDRESS                            TUNNEL-ID    TYPE    ORIGIN    STATUS
-------------------------------------------------------------------------------------------------------
2011:beef:3:0:0:0:0:67                  T-1          UNICAST MANUAL    PREFERRED
fe80:0:0:0:0:0:4301:101                 T-1          UNICAST LINKLAYER PREFERRED
2011:beef:4:0:0:0:0:67                  T-2          UNICAST MANUAL    PREFERRED
fe80:0:0:0:0:0:4301:101                 T-2          UNICAST LINKLAYER PREFERRED

2 out of 10 Total Num of Interface Entries displayed.
4 out of 20 Total Num of Address Entries displayed.
```

```
Switch:1#show ipv6 address interface tunnel 2

==========================================================================================
                                   Address Information
==========================================================================================
IPV6 ADDRESS/PREFIX LENGTH                   VID/BID/TID  TYPE    ORIGIN    STATUS
------------------------------------------------------------------------------------------
44:211:0:0:0:0:0:2/64                        T-2          UNICAST MANUAL    PREFERRED
fe80:0:0:0:0:0:d301:3702/64                  T-2          UNICAST LINKLAYER PREFERRED

2 out of 407 Total Num of Address Entries displayed.
```

```
Switch:1#show ipv6 address interface vlan 100

==========================================================================================
                                   Address Information
==========================================================================================
IPV6 ADDRESS/PREFIX LENGTH                   VID/BID/TID  TYPE    ORIGIN    STATUS
------------------------------------------------------------------------------------------
10:1:50:0:0:0:0:7/64                         V-100        UNICAST MANUAL    PREFERRED
fe80:0:0:0:b2ad:aaff:fe46:f19a/64            V-100        UNICAST LINKLAYER PREFERRED

2 out of 407 Total Num of Address Entries displayed.
```

```
Switch:1#show ipv6 forwarding
        Global forwarding              : enable
        ecmp                           : disable
        ecmp-max-path                  : 1
```

```
Switch:1#show ipv6 global
        forwarding                     : enable
        default-hop-cnt                : 64
        number-of-interfaces           : 11
        icmp-error-interval            : 1000
        icmp-error-quota               : 50
        icmp-unreach-msg               : disable
        icmp-redirect-msg              : disable
        static-route-admin-status      : enable
        ecmp                           : enable
        ecmp-max-path                  : 4
        source-route                   : disable
```

```
Switch:1#show ipv6 nd interface vlan

===================================================================================================
                                             Vlan Ipv6 Nd
===================================================================================================
IFID VLAN   RTR-ADV MAX-INT MIN-INT LIFETIME MANAG OTHER DAD-NS MTU   HOP    REACHABLE RETRANSMIT
                                             FLAG  CONF               LIMIT  TIME      TIME
----------------------------------------------------------------------------------------------------
2148 V-100  True    600     200     1800     False False  1    0(d)    64(d)  0(d)       0(d)
2158 V-110  True    600     200     1800     False False  1    0(d)    64(d)  0(d)       0(d)
2248 V-200  True    600     200     1800     False False  1    0(d)    64(d)  0(d)       0(d)
2258 V-210  True    600     200     1800     False False  1    0(d)    64(d)  0(d)       0(d)
2548 V-500  True    600     200     1800     False False  1    0(d)    64(d)  0(d)       0(d)
2648 V-600  True    600     200     1800     False False  1    0(d)    64(d)  0(d)       0(d)
2948 V-900  True    600     200     1800     False False  1    0(d)    64(d)  0(d)       0(d)

Note:  (s) = Set, (d) = Default, (i) = inherit.

7 out of 11 Total Num of Ipv6 ND Entries displayed.
```

```
Switch:1#show ipv6 nd interface mgmtEthernet mgmt
=============================================================================================
==========
                                             Mgmt Ipv6 Nd
=============================================================================================
==========
IFID MGMT-IF RTR-ADV MAX-INT MIN-INT LIFETIME MANAG OTHER DAD-NS MTU     HOP    REACHABLE
RETRANSMIT
                                             FLAG  CONF                 LIMIT  TIME
TIME
---------------------------------------------------------------------------------------------
----------
64   mgmt   False   600     200     1800     False False 1      0(d)    64(d)  0(d)
0(d)
```

```
Switch:1#show ipv6 nd-prefix interface gigabitethernet

====================================================================================
                              Port Ipv6 Nd Prefix
====================================================================================
INTF  IPV6                                          BTR   VALID       PREF     EUI
INDEX ADDRESS/PREFIX                                      LIFE        LIFE
------------------------------------------------------------------------------------
344   2011:beef:4004:0:0:0:0:0/64                      5/25   2592000    604800 1

1 out of 9 Total Num of Ipv6 ND prefix Entries displayed.
```

```
Switch:1#show ipv6 nd-prefix interface vlan

====================================================================================
                              Vlan Ipv6 Nd Prefix
====================================================================================
INTF  IPV6                                          VLAN  VALID       PREF EUI
INDEX ADDRESS/PREFIX                                ID    LIFE        LIFE
------------------------------------------------------------------------------------
2148  2011:beef:100:0:0:0:0:0/64                    100   2592000     604800 1
2158  2011:beef:110:0:0:0:0:0/64                    110   2592000     604800 1
2248  2011:beef:200:0:0:0:0:0/64                    200   2592000     604800 1
2258  2011:beef:210:0:0:0:0:0/48                    210   2592000     604800 1
2548  2011:beef:500:0:0:0:0:0/64                    500   2592000     604800 1
2648  2011:beef:600:0:0:0:0:0/64                    600   2592000     604800 1
2948  2011:beef:900:0:0:0:0:0/64                    900   2592000     604800 1

7 out of 9 Total Num of Ipv6 ND prefix Entries displayed.
```

```
Switch:1#show ipv6 nd-prefix vlan 100

================================================================================
                         Nd-Prefix Address Information
================================================================================
INTF  IPV6                                           VLAN  VALID    PREF     EUI
INDEX ADDRESS/PREFIX                                 ID    LIFE     LIFE
--------------------------------------------------------------------------------
2148  2011:beef:100:0:0:0:0:0/64                     100   2592000  604800   1
--------------------------------------------------------------------------------
Legend: EUI: eui-not-used(1), eui-used-with-ul-complement(2)eui-used-without-ul-complement(3)
```

```
Switch:1#show ipv6 neighbor type 2

================================================================================
                              Neighbor Information
================================================================================
NET ADDRESS/                   IPV6   PHYS    TYPE    STATE      LAST
PHYSICAL ADDRESS               INTF   INTF                       UPD
--------------------------------------------------------------------------------
2013:47:17:120:0:0:0:1/        1/1    1/1   DYNAMIC REACHABLE  5640 00:1d:af:64:a2:01
2013:47:17:120:0:0:0:2/        1/1    1/1   DYNAMIC STALE      5170 00:18:b0:5a:92:01
2013:47:17:120:1:0:0:7/        1/1    1/1   DYNAMIC STALE      5321 80:17:7d:76:63:fd
2013:47:17:120:1:0:0:23/       1/1    1/1   DYNAMIC STALE      5126 00:24:7f:a1:63:fd
2013:47:17:120:1:0:0:231/      1/1    1/1   DYNAMIC STALE      5398 80:17:7d:76:63:ff
2013:47:17:120:1:0:0:233/      1/1    1/1   DYNAMIC STALE      5195 80:17:7d:75:93:ff
2013:47:17:120:1:0:0:239/      1/1    1/1   DYNAMIC STALE      5207 80:17:7d:75:93:fd
2013:47:17:120:1:0:0:243/      1/1    1/1   DYNAMIC STALE      5190 00:24:7f:a1:63:ff

--More-- (q = quit)
```

```
Switch:1(config)#show ipv6 neighbor

================================================================================
                              Neighbor Information
================================================================================
NET ADDRESS/                             IPV6   PHYS    TYPE    STATE      LAST
PHYSICAL ADDRESS                         INTF   INTF                       UPD
--------------------------------------------------------------------------------
2013:47:17:120:0:0:0:1/                  1/1    1/1     DYNAMIC STALE      5681
00:1d:af:64:a2:01
2013:47:17:120:0:0:0:2/                  1/1    1/1     DYNAMIC STALE      5170
00:18:b0:5a:92:01
2013:47:17:120:1:0:0:7/                  1/1    1/1     DYNAMIC STALE      5321
80:17:7d:76:63:fd
2013:47:17:120:1:0:0:23/                 1/1    1/1     DYNAMIC STALE      5126
00:24:7f:a1:63:fd
2013:47:17:120:1:0:0:231/                1/1    1/1     DYNAMIC STALE      5398
80:17:7d:76:63:ff
2013:47:17:120:1:0:0:233/                1/1    1/1     DYNAMIC STALE      5195
80:17:7d:75:93:ff
2013:47:17:120:1:0:0:239/                1/1    1/1     DYNAMIC STALE      5207
80:17:7d:75:93:fd
2013:47:17:120:1:0:0:243/                1/1    1/1     DYNAMIC STALE      5190
00:24:7f:a1:63:ff

--More-- (q = quit)
```

Variable definitions

Use the data in the following table to use the **`show ipv6`** commands.

Variable	Value
address interface ip *WORD<0-46>*	Specifies the IPv6 address.
neighbor [*WORD<0-46>*]	Specifies the IPv6 address of the neighbor.
loopback <1-256>	Specifies the loopback interface ID value. If you do not specify a value, the output includes all IPv6 loopback interfaces.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).
type *<1–4>*	Specifies the neighbor type as one of the following: • 1 - other

Table continues…

Variable	Value
	• 2 - dynamic • 3 - static • 4 - local
tunnel <*1–2000*>	Specifies the tunnel ID.
vlan <*1-4059*>	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

Viewing cached destination information

View the destination cache to see next-hop addresses for destinations.

The destination cache is only populated or updated when IPv6 packets originate locally on the central processor of the switch.

The main purpose of the destination cache is to store, on a per-destination basis, the dynamic Path MTU value currently used when transmitting packets from the local system to the remote destination.

The system uses the PMTU value to calculate how many bytes can fit into an individual packet before fragmentation should be applied.

About this task

The command output shows the following information:

- the IPv6 destination address
- the IPv6 address for the next hop to the destination
- the path maximum transmission unit (MTU) for the destination
- the time, in seconds, since an ICMPv6 packet-too-big message was received

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View the destination cache for all interfaces:

   ```
   show ipv6 dcache
   ```
3. View the destination cache for a brouter port:

   ```
   show ipv6 dcache gigabitethernet {slot/port[sub-port]}
   ```
4. View the destination cache for a management port:

   ```
   show ipv6 dcache mgmtethernet mgmt
   ```

Note:

This step only applies to hardware with a dedicated, physical management interface.

5. View the destination cache for a specific tunnel ID:

   `show ipv6 dcache tunnel <1-2000>`

6. View the destination cache for a VLAN:

   `show ipv6 dcache vlan <1-4059>`

7. Clear the destination cache:

   ```
   clear ipv6 dcache [gigabitethernet {slot/port[sub-port]}]
   [mgmtethernet {slot/port[sub-port]}][tunnel <1-2000>][vlan
   <1-4059> ]
   ```

Example

```
Switch:1(config-if)#show ipv6 dcache
=============================================================================
                      IPv6 Destination Cache Information
=============================================================================
Destination Address NEXT HOP         VID/BID/TID  IF_TYPE   IF_DATA  PMTU PMTU_
                                                                          AGE
-----------------------------------------------------------------------------
2:0:0:0:0:0:0:36    0:0:0:0:0:0:0:0  V-2          real      -        1500  0
3:0:0:0:0:0:0:36    0:0:0:0:0:0:0:0  V-3          real      -        1500  0
4:0:0:0:0:0:0:36    0:0:0:0:0:0:0:0  V-4          real      -        1500  0
ff02:0:0:0:0:0:0:1  0:0:0:0:0:0:0:0  6/7          real      -        1500  0
ff02:0:0:0:0:0:0:1  0:0:0:0:0:0:0:0  V-2          real      -        1500  0
ff02:0:0:0:0:0:0:1  0:0:0:0:0:0:0:0  V-3          real      -        1500  0
ff02:0:0:0:0:0:0:1  0:0:0:0:0:0:0:0  V-4          real      -        1500  0
ff02:0:0:0:0:0:0:1  0:0:0:0:0:0:0:0  T-25         real      -        1280  0
ff02:0:0:0:0:0:0:1  0:0:0:0:0:0:0:0  V-2          virtual   rsmlt    1500  0
ff02:0:0:0:0:0:0:1  0:0:0:0:0:0:0:0  V-3          virtual   vrId-1   1500  0
ff02:0:0:0:0:0:0:1  0:0:0:0:0:0:0:0  V-4          virtual   vrId-1   1500  0
ff02:0:0:0:0:0:0:1  0:0:0:0:0:0:0:0  V-4          virtual   vrId-10  1500  0
ff02:0:0:0:0:0:0:1  0:0:0:0:0:0:0:0  V-3          virtual   vrId-255 1500  0
ff02:0:0:0:0:0:0:12 0:0:0:0:0:0:0:0  V-3          virtual   vrId-1   1500  0
ff02:0:0:0:0:0:0:12 0:0:0:0:0:0:0:0  V-4          virtual   vrId-1   1500  0
ff02:0:0:0:0:0:0:12 0:0:0:0:0:0:0:0  V-4          virtual   vrId-10  1500  0
ff02:0:0:0:0:0:0:12 0:0:0:0:0:0:0:0  V-3          virtual   vrId-255 1500  0
ff02:0:0:0:0:0:0:16 0:0:0:0:0:0:0:0  V-2          real      -        1500  0
ff02:0:0:0:0:0:0:16 0:0:0:0:0:0:0:0  V-3          real      -        1500  0
ff02:0:0:0:0:0:0:16 0:0:0:0:0:0:0:0  V-4          real      -        1500  0
ff02:0:0:0:0:0:0:16 0:0:0:0:0:0:0:0  T-25         real      -        1280  0
ff02:0:0:0:0:0:0:16 0:0:0:0:0:0:0:0  V-2          virtual   rsmlt    1500  0
ff02:0:0:0:0:0:0:16 0:0:0:0:0:0:0:0  V-3          virtual   vrId-1   1500  0
ff02:0:0:0:0:0:0:16 0:0:0:0:0:0:0:0  V-4          virtual   vrId-1   1500  0
ff02:0:0:0:0:0:0:16 0:0:0:0:0:0:0:0  V-4          virtual   vrId-10  1500  0
ff02:0:0:0:0:0:0:16 0:0:0:0:0:0:0:0  V-3          virtual   vrId-255 1500  0
-----------------------------------------------------------------------------
```

Variable definitions

Use the data in the following table to use the **`show ipv6 dcache`** and **`clear ipv6 dcache`** commands.

Variable	Value
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
{slot/port}	Identifies a single slot and port.

Entity MIB – Physical Table

Use the information in the following sections to understand the Entity MIB – Physical Table.

Entity MIB – Physical Table

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

Some hardware platforms support removable interface modules while others offer a fixed configuration. The names used for these modules can vary depending on the hardware platform.

The following table identifies the entity index range for the switch components.

Component	Entity index range
Chassis	1
Power supply slot	2 to 7
Fan tray and fan slot	8 to 15
I/O slot	16 to 35
I/O card or module	36 to 55
Console port	56
Management port	57
Power supply	68 to 73
Fan tray	74 to 81
Fan module	82 to 105

For more information about Entity MIB – Physical Table, see Viewing physical entities on page 27.

Viewing physical entities

Perform this procedure to view information about the functional components of the switch.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.
2. Click **Entity**.

Physical Entities field descriptions

Use the following table to use the Physical Entities tab.

Name	Description
Index	Indicates the index of the entry.
Descr	Indicates the name of the manufacturer for the physical entity.
VendorType	Indicates the vendor-specific hardware type for the physical entity. Because there is no vendor-specifier registration for this device, the value is 0.
ContainedIn	Indicates the index value for the physical entity which contains this physical entity. A value of zero indicates that this physical entity is not contained in any other physical entity.
Class	Indicates the general hardware type of the physical entity. The value is configured to the standard enumeration value that indicates the general class of the physical entity.
ParentRelPos	Indicates the relative position of the child component among the sibling components.
Name	Indicates the name of the component, as assigned by the local device, and that is suitable to use in commands you enter on the console of the device. Depending on the physical component naming syntax of the device, the name can be a text name such as console, or a component number such as port or module number. If there is no local name, there is no value.
HardwareRev	Indicates the vendor-specific hardware revision string for the physical entity. If no specific hardware revision string is associated with the physical component, or if this information is unknown, then this object contains a zero-length string, or there is no value. If there is no information available, there is no value.
FirmwareRev	Indicates the vendor-specific firmware revision string for the physical entity.

Table continues…

Name	Description
	If no specific firmware programs are associated with the physical component, or if this information is unknown, then this object contains a zero-length string, or there is no value. If there is no information available, there is no value.
SoftwareRev	Indicates the vendor-specific software revision string for the physical entity. If no specific software programs are associated with the physical component, or if this information is unknown, then this object contains a zero-length string, or there is no value. If there is no information available, there is no value.
SerialNum	Indicates the vendor-specific serial number string for the physical entity. The value is the serial number string printed on the component, if present. If there is no information available, there is no value.
MfgName	Indicates the name of the manufacturer of the physical component. The value is the manufacturer name string printed on the component, if present. If the manufacturer name string associated with the physical component is unknown, then this object contains a zero-length string. If there is no information available, there is no value.
ModelName	Indicates the vendor-specific model name identifier string associated with the physical component. The value is the part number which is printed on the component. If the model name string associated with the physical component is unknown, then this object contains a zero-length string.
Alias	Indicates an alias name for the physical entity that is specified by a network manager, and provides a nonvolatile handle for the physical entity. The software supports read-only and provides values for the port interface only.
AssetID	Indicates a user-assigned asset tracking identifier for the physical entity. This value is specified by a network manager, and provides nonvolatile storage of this information. Because this object is not supported, there is no value.

Table continues…

Name	Description
IsFRU	Indicates whether or not the physical entity is considered a field replaceable unit. • If the value is `true(1)`, then the component is a field replaceable unit. • If the value is `false(2)`, then the component is permanently contained within a field replaceable unit.
MfgDate	Indicates the manufacturing date of the managed entity. If the manufacturing date is unknown, then the value is `'0000000000000000'H`.
Uris	Indicates additional identification information about the physical entity. **Uris** is not supported, therefore there is no value.

IEEE 802.3X Pause frame transmit

Use the information in the following sections to understand IEEE 802.3X Pause frame transmit and its configuration using the CLI or the EDM.

IEEE 802.3X Pause frame transmit

The switch uses MAC pause frames to provide congestion relief on full-duplex interfaces.

Overview

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

The switch generates pause frames to tell the sending device to stop sending additional packets for a specified time period. After the time period expires, the sending device can resume sending packets. During the specified time period, if the switch determines the congestion is reduced, it can send pause frames to the sending device to instruct it to begin sending packets immediately.

Flow control mode and pause frames

If you enable flow control mode globally, the switch drops packets on ingress when congestion occurs. If the switch is not in flow control mode, it drops packets at egress when congestion occurs.

Configure an interface to send pause frames when congestion occurs to alleviate packet drops due to flow control mode.

Auto-Negotiation

Interfaces that support auto-negotiation advertise and exchange their flow control capability to agree on a pause frame configuration. IEEE 802.3 annex 28b defines the auto-negotiation ability fields and the pause resolution. The switch advertises only two capabilities. The following table shows the software bit settings based on the flow control configuration.

Note:

Not all interfaces support Auto-Negotiation. For more information, see your hardware documentation.

Table 3: Advertised abilities

Interface configuration	Pause	ASM	Capability advertised
Flow control enabled	1	0	Symmetric pause
Flow control disabled	1	1	Both Symmetric pause and asymmetric pause

The following tables identifies the pause resolution.

Table 4: Pause resolution

Local device pause	Local device ASM	Peer device pause	Peer device ASM	Local device resolution	Peer device resolution
0	0	Do not care	Do not care	Disable pause transmit and receive.	Disable pause transmit and receive.
0	1	0	Do not care	Disable pause transmit and receive.	Disable pause transmit and receive.
0	1	1	0	Disable pause transmit and receive.	Disable pause transmit and receive.
0	1	1	1	Enable pause transmit. Disable pause receive.	Disable pause transmit. Enable pause receive.
1	0	0	Do not care	Disable pause transmit and receive.	Disable pause transmit and receive.
1	Do not care	1	Do not care	Enable pause transmit and receive.	Enable pause transmit and receive.
1	1	0	0	Disable pause transmit and receive.	Disable pause transmit and receive.

Table continues…

Local device pause	Local device ASM	Peer device pause	Peer device ASM	Local device resolution	Peer device resolution
1	1	0	1	Disable pause transmit. Enable pause receive.	Enable pause transmit. Disable pause receive.

The following list identifies the type of interfaces that support auto-negotiated flow control:

- 10 Mbps/100 Mbps/1 Gbps copper
- 100 Mbps/1 Gbps/10 Gbps copper
- 1 Gbps fiber (in both SFP and SFP+ ports)

Configuring Layer 2 flow control

Configure Layer 2 flow control to eliminate or minimize packet loss.

About this task

By default, flow control mode is disabled. When disabled, the system does not generate nor configure the transmission of flow control messages. The system always honors received flow control messages regardless of the flow control mode status. You must enable this mode before you configure an interface to send pause frames.

By default, an interface does not send pause frames.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable flow control mode:

   ```
   boot config flags flow-control-mode
   ```

3. Save the configuration.
4. Exit Privileged EXEC mode:

   ```
   exit
   ```

5. Reboot the chassis.

   ```
   boot
   ```

6. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

7. Configure the interface to generate pause frames:

```
tx-flow-control [enable]
```

8. **(Optional)** Configure other interfaces to generate pause frames:

   ```
   tx-flow-control port {slot/port[/sub-port] [-slot/port[/sub-port]]
   [,...]} enable
   ```

9. Verify the boot flag configuration:

   ```
   show boot config flags
   ```

10. Verify the interface configuration:

    ```
    show interfaces gigabitEthernet l1-config {slot/port[/sub-port] [-
    slot/port[/sub-port]] [,...]}
    ```

11. View the pause-frame packet count:

    ```
    show interfaces gigabitEthernet statistics {slot/port[/sub-port] [-
    slot/port[/sub-port]] [,...]}
    ```

Example

Enable flow control on the system and configure slot 1, port 10 to send pause frames. Verify the configuration.

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#boot config flags flow-control-mode
Warning: Please save the configuration and reboot the switch
         for this configuration to take effect.
Switch:1<config>#save config
CP-1: Save config to file /intflash/config.cfg successful.
CP-1: Save license to file /intflash/license.xml successful.
Switch:1<config>#exit
Switch:1#boot
Are you sure you want to re-boot the switch (y/n) ?y
```

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#interface gigabitethernet 1/10
Switch:1(config-if)#tx-flow-control enable
Switch:1(config-if)#show boot config flags
flags block-snmp false
flags debug-config false
flags debugmode false
flags enhancedsecure-mode false
flags factorydefaults false
flags flow-control-mode true
flags ftpd true
flags hsecure false
flags ipv6-mode false
flags logging true
flags reboot true
flags rlogind false
flags spanning-tree-mode mstp
flags spbm-bandwidth-reservation false
flags sshd false
flags telnetd true
flags tftpd false
```

```
flags trace-logging false
flags verify-config true
```

```
Switch:1(config-if)#show interfaces gigabitEthernet l1-config 1/10
================================================================================
                                      Port Config L1
================================================================================
PORT     AUTO  CUSTOM AUTO NEGOTIATION    ADMIN      OPERATE    ADMIN         OPERATE
NUM      NEG.  ADVERTISEMENTS             DPLX  SPD  DPLX  SPD  TX-FLW-CTRL   TX-FLW-CTRL
--------------------------------------------------------------------------------
1/10     true Not Configured             full 10000       0    enable       enable
```

View the pause-frame packet count for slot 1, port 10.

```
Switch:1(config-if)#show interfaces gigabitEthernet statistics 1/10
============================================================================================
                                          Port Stats Interface
============================================================================================
PORT     IN             OUT                  IN                   OUT
NUM    OCTETS          OCTETS               PACKET               PACKET
--------------------------------------------------------------------------------------------
1/1    29964704384     22788614528          234106526            178034166

PORT     IN             OUT                 IN                   OUT            OUTLOSS
NUM    FLOWCTRL        FLOWCTRL            PFC                  PFC            PACKETS
--------------------------------------------------------------------------------------------
1/1    0               11014               0                    0             0
```

Variable definitions

Use the data in the following table to use the **`tx-flow-control`** command.

Variable	Value
enable	Configures the interface to send pause frames. By default, flow control is disabled.
port *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

Use the data in the following table to use the **`show interfaces gigabitEthernet l1-config`** and **`show interfaces gigabitEthernet statistics`** commands.

Variable	Value
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

Configuring IEEE 802.3X Pause frame transmit

Configure IEEE 802.3X Pause frame transmit to eliminate or minimize packet loss.

About this task

By default, flow control mode is disabled. When disabled, the system does not generate nor configure the transmission of flow control messages. The system always honors received flow control messages regardless of the flow control mode status. You must enable this mode before you configure an interface to send pause frames.

By default, an interface does not send pause frames.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.
2. Click **Chassis**.
3. Click the **Boot Config** tab.
4. For EnableFlowControlMode, select **enable**.
5. Click **Apply**.
6. Save the switch configuration.
7. Reboot the chassis, and log in again.
8. In the Device Physical View, select a port or ports.
9. In the navigation pane, expand the **Configuration** > **Edit** > **Port** folders.
10. Click **General**.
11. Click the **Interface** tab.
12. For TxFlowControl, select **enable** to enable the interface to generate pause frames.
13. Click **Apply**.

Viewing port interface statistics

View port interface statistics to manage network performance.

Procedure

1. In the Device Physical View, select a port.
2. In the navigation pane, expand the **Configuration** > **Graph** folders.
3. Click **Port**.
4. Click the **Interface** tab.

Interface field descriptions

The following table describes parameters on the Interface tab.

Name	Description
InOctets	Specifies the number of octets received on the interface, including framing characters.
OutOctets	Specifies the number of octets transmitted from the interface, including framing characters.
InUcastPkts	Specifies the number of packets delivered by this sublayer to a higher sublayer that were not addressed to a multicast or broadcast address at this sublayer.
OutUcastPkts	Specifies the number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast address at this sublayer. The total number includes those packets discarded or not sent.
InMulticastPkts	Specifies the number of packets delivered by this sublayer to a higher sublayer that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both group and functional addresses.
OutMulticastPkts	Specifies the number of packets that higher-level protocols requested be transmitted, and that are addressed to a multicast address at this sublayer, including those that were discarded or not sent. For a MAC layer protocol, this number includes both group and functional addresses.
InBroadcastPkts	Specifies the number of packets delivered by this sublayer to a higher sublayer that are addressed to a broadcast address at this sublayer.
OutBroadcastPkts	Specifies the number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this sublayer, including those that were discarded or not sent.
InDiscards	Specifies the number of inbound packets that are discarded because of frames with errors or invalid frames or, in some cases, to fill up buffer space.
InErrors	For packet-oriented interfaces, specifies the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
InUnknownProtos	For packet-oriented interfaces, specifies the number of packets received through the interface that are discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received through the interface that were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter is always 0.
HCInPfcPkts	Specifies the total number of Priority Flow Control (PFC) packets received by this interface. This number does not increment for port-level flow control.

Table continues…

Name	Description
HCOutPfcPkts	Specifies the total number of PFC packets transmitted by this interface. This number does not increment for port-level flow control.
InFlowCtrlPkts	Specifies the number of port-level flow control packets received by this interface.
OutFlowCtrlPkts	Specifies the number of port-level flow control packets transmitted by this interface.
InPfcPkts	Specifies the total number of port-level flow control packets received by this interface.
OutPfcPkts	Specifies the total number of port-level flow control packets transmitted by this interface.
NumStateTransition	Specifies the number of times the port went in and out of service; the number of state transitions from up to down.

Link Layer Discovery Protocol (LLDP)

Use the information in the following sections to understand LLDP and its configuration using the CLI or the EDM.

Link Layer Discovery Protocol (802.1AB) fundamentals

With Link Layer Discovery Protocol (LLDP) you can obtain node and topology information to help detect and correct network and configuration errors.

LLDP

802.1AB is the IEEE standard called Station and Media Access Control Connectivity Discovery. This standard defines the Link Layer Discovery Protocol.

LLDP stations connected to a local area network (LAN) can advertise station capabilities to each other, allowing the discovery of physical topology information for network management.

LLDP-compatible stations can comprise any interconnection device, including PCs, IP Phones, switches, and routers.

Each LLDP station stores LLDP information in a standard Management Information Base (MIB), making it possible for a network management system (NMS) or application to access the information.

The functions of an LLDP station include:

- Advertising connectivity and management information about the local station to adjacent stations
- Receiving network management information from adjacent stations
- Enabling the discovery of certain configuration inconsistencies or malfunctions that can result in impaired communications at higher layers

For example, you can use LLDP to discover duplex mismatches between an IP Phone and the connected switch.

LLDP is compatible with IETF PROTO MIB (IETF RFC 2922).

The following figure shows an example of a LAN using LLDP.

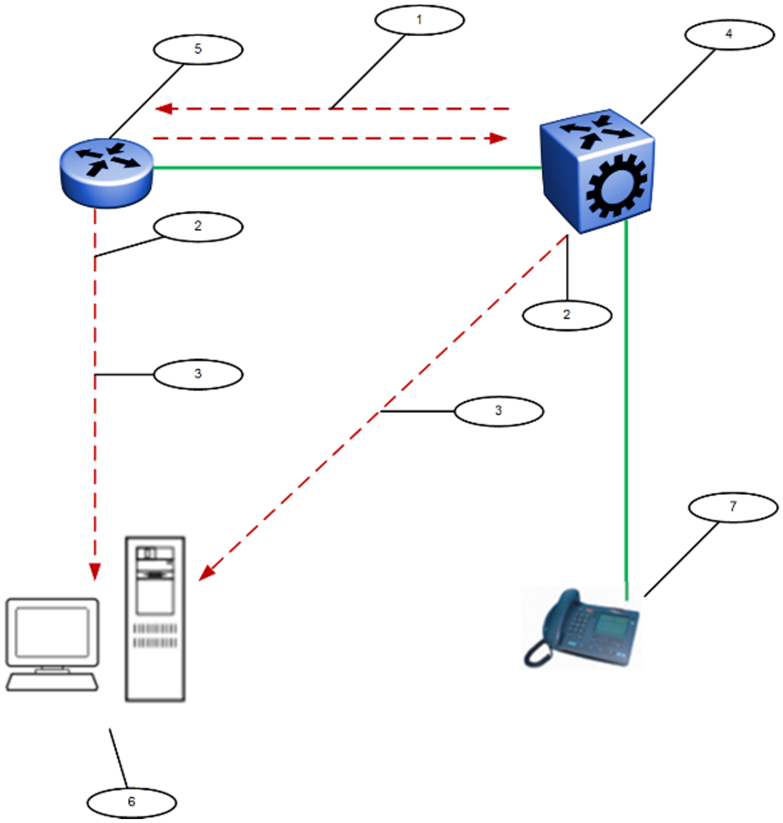


Figure 1: LLDP in a LAN

Legend:

1. The switch and an LLDP-enabled router advertise chassis and port IDs and system descriptions to each other
2. The devices store the information about each other in local MIB databases, accessible with SNMP
3. A network management system retrieves the data stored by each device and builds a network topology map
4. Switch
5. Router
6. Management work station
7. IP Phone

LLDP modes

LLDP is a one-way protocol.

An LLDP agent can transmit information about the capabilities and current status of the system associated with its MAC service access point (MSAP) identifier.

The LLDP agent also can receive information about the capabilities and current status of the system associated with a remote MSAP identifier.

However, LLDP agents cannot solicit information from each other.

Modes:

You can configure the local LLDP agent to

- Transmit and receive

Connectivity and management information

The information parameters in each LLDP frame are in a Link Layer Discovery Protocol Data Unit (LLDP PDU) as a sequence of short, variable length information elements known as TLVs (type, length, value).

Each LLDP PDU includes the following mandatory TLVs:

- Chassis ID
- Port ID
- Time To Live
- Port Description
- System Name
- System Description
- System Capabilities (indicates both the system supported capabilities and enabled capabilities, such as end station, bridge, or router)
- Management Address

The chassis ID and the port ID values are concatenated to form a logical MSAP identifier that the recipient uses to identify the sending LLDP agent and port.

A non-zero value in the Time to Live (TTL) field of the TTL TLV indicates to the receiving LLDP agent how long the LLDP PDU information from the MSAP identifier remains valid.

The receiving LLDP agent automatically discards all LLDP PDU information, if the sender fails to update it in a timely manner.

A zero value in TTL field of Time To Live TLV tells the receiving LLDP agent to discard the information associated with the LLDP PDU MSAP identifier.

Transmitting LLDP PDUs

When a transmit cycle is initiated, the LLDP manager extracts the managed objects from the LLDP local system MIB and formats this information into TLVs. TLVs are inserted into the LLDP PDU.

LLDP PDUs are regularly transmitted at a user-configurable transmit interval (tx-interval) or when any of the variables in the LLPDU is modified on the local system; for example, system name or management address.

Transmission delay (tx-delay) is the minimum delay between successive LLDP frame transmissions.

TLV system MIBs

The LLDP local system MIB stores the information to construct the various TLVs for transmission.

The LLDP remote systems MIB stores the information received from remote LLDP agents.

LLDP PDU and TLV error handling

The system discards LLDP PDUs and TLVs that contain detectable errors.

The system assumes that TLVs that contain no basic format errors, but that it does not recognize, are valid and stores them for retrieval by network management.

LLDP and MultiLink Trunking

You must apply TLVs on a per-port basis.

Because LLDP manages trunked ports individually, TLVs configured on one port in a trunk do not propagate automatically to other ports in the trunk.

And the system sends advertisements to each port in a trunk, not on a per-trunk basis.

LLDP and Fabric Attach

Fabric Attach uses LLDP to signal a desire to join the SPB network. When a switch is enabled as an FA Server, it receives IEEE 802.1AB LLDP messages from FA Client and FA Proxy devices requesting the creation of Switched UNI service identifiers (I-SIDs). All of the discovery handshakes and I-SID mapping requests are using LLDP TLV fields. Based on the LLDP standard, FA information is transmitted using organizational TLVs within LLDP PDUs.

FA also leverages LLDP to discover directly connected FA peers and to exchange information associated with FA between those peers.

Link Layer Discovery Protocol configuration using CLI

This section describes how to configure Link Layer Discovery Protocol using the Command Line Interface (CLI).

IPv4 management IP addresses are supported by LLDP, including the management virtual IP address, and they are advertised in the Management address TLV.

Configuring global LLDP transmission parameters

Before you begin

- In the GigabitEthernet Interface Configuration mode, specify the LLDP port status as transmit only or transmit and receive.

About this task

Use this procedure to configure global LLDP transmission parameters on the switch. If required, you can also restore these parameters to their default values.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. To configure the LLDP transmission parameters, enter:

   ```
   lldp [tx-interval|tx-hold-multiplier]
   ```

3. **(Optional)** To restore specific LLDP transmission parameters to their default values, enter:

   ```
   default lldp [tx-interval|tx-hold-multiplier]
   ```

4. **(Optional)** To restore all LLDP transmission parameters to their default values, enter:

   ```
   default lldp
   ```

Example

Configure the LLDP transmission interval. The LLDP port status is set to transmit and receive prior to the configuration.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 4/4
Switch:1(config-if)#lldp status txAndRx
Switch:1(config-if)#exit
Switch:1(config)#lldp tx-interval 31
```

Optionally, restore the LLDP transmission interval to its default value:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#default lldp tx-interval
```

Variable definitions

Use the information in the following table to help you understand the **`lldp`** command.

Variable	Value
tx-interval<*5–32768*>	Specifies the global LLDP transmit interval in seconds, that is, the interval in which LLDP frames are transmitted. The default is 30 seconds.
tx-hold-multiplier <*2–10*>	Configures the multiplier for the transmit interval used to compute the Time To Live (TTL) value in LLDP frames. The default is 4 seconds.

Configuring LLDP status on ports

About this task

Use this procedure to configure LLDP and configure the status to transmit and receive on a port, or ports, on your switch.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

```
enable

configure terminal
```

2. To configure LLDP and configure the status for transmit and receive on a port or ports, enter:

   ```
   lldp port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
   status <txAndRx>
   ```

3. To configure LLDP to the default setting for a port or ports, enter:

   ```
   default lldp port {slot/port[/sub-port] [-slot/port[/sub-port]]
   [,...]} status <txAndRx>
   ```

Example

Configure LLDP on your switch and set the status for transmit and receive on a port:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 4/4
Switch:1(config-if)#lldp status txAndRx
```

Restore LLDP port status to the default value. The default status is *disabled*.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 4/4
Switch:1(config-if)#default lldp status
```

Disable LLDP on your switch:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 4/4
Switch:1(config-if)#no lldp status
```

Variable definitions

Use the data in the following table to use the **`lldp port`** command.

Variable	Value
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).
status <*txAndRx*>	Configures the LLDP Data Unit (LLDP PDU) transmit and receive status on the port(s). • default—restores LLDP port parameters to default values • txAndrx—enables LLDP PDU transmit and receive

Enabling CDP mode on a port

In order to use CDP compatible mode, you must enable it on a port, or ports, on your switch.

If CDP is enabled, the interface accepts only CDP packets. Similarly, if CDP is disabled but LLDP is enabled, the interface accepts only LLDP packets.

To switch a port from CDP mode to LLDP mode, the LLDP status on that port must be txAndrx.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. At the prompt, enter the following command:

   ```
   [no] [default] lldp port <portlist> status <txAndrx>
   ```

3. To enable CDP, enter the following command:

   ```
   [no] lldp cdp enable
   ```

Example

To enable CDP on a port:

```
Switch:1>enable
Switch:1>#config t
Switch:1>(config)#interface GigabitEthernet 4/4
Switch:1>(config-if)#lldp status txAndRx
Switch:1>(config-if)#lldp cdp enable
```

To switch a port from cdp mode to lldp mode

Note:

lldp status on that port must be txAndrx

```
Switch:1>enable
Switch:1>#config t
Switch:1>(config)#interface GigabitEthernet 4/4
Switch:1>(config-if)#no lldp cdp enable
```

To shutdown lldp or cdp on a port:

```
Switch:1>enable
Switch:1>#config t
Switch:1>(config)#interface GigabitEthernet 4/4
Switch:1>(config-if)#no lldp status
```

To display LLDP neighbors while in CDP mode

```
Switch:1>enable
Switch:1>#config t
Switch:1>(config)#interface GigabitEthernet 4/4
Switch:1>(config-if)#lldp status txAndRx
Switch:1>(config-if)#lldp cdp enable
```

Variable definitions

Use the information in the following table to help you understand the **[no] [default] lldp cdp enable** command.

Variable	Value
port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
[no] [default]	Enables CDP on the port. • no—disables LLDP on the port • default—restores LLDP port parameters to default values The default is disabled.

Viewing global LLDP information

About this task

Use this procedure to view global LLDP information, to know which LLDP settings and parameters are configured.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To verify global LLDP information, enter:

   ```
   show lldp {local-sys-data|[neighbor port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]|[port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}] |[rx-stats port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]|[stats]|[tx-stats port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]}
   ```

Example

View global LLDP information:

```
Switch:1#show lldp
802.1ab Configuration:
------------------------------------
             TxInterval: 30
       TxHoldMultiplier: 4
            ReinitDelay: 1
                TxDelay: 1
   NotificationInterval: 5
```

View the LLDP local system data on the switch:

```
Switch:1#show lldp local-sys-data

======================================================================
                             LLDP Local System Data

======================================================================
```

```
               ChassisId: MAC Address        b0:ad:aa:4c:54:00
               SysName  : LLDP agent
               SysDescr : <model-name> (<release-number>)  BoxType: <model-name>
               SysCap   : Br / Br
----------------------------------------------------------------------
Capabilities Legend: (Supported/Enabled)
B= Bridge,    D= DOCSIS,    O= Other,     R= Repeater,
S= Station,   T= Telephone, W= WLAN,      r= Router
```

View the LLDP neighbor information. You can also view this on a specific port.

```
Switch:1#show lldp neighbor

===============================================================================
                                      LLDP Neighbor
===============================================================================

Port: 1/28      Index    : 1                   Time: 0 day(s), 01:16:25
                Protocol : LLDP
                ChassisId: MAC Address         a4:25:1b:52:54:00
                PortId   : MAC Address         a4:25:1b:52:54:1b
                SysName  : BEB
                SysCap   : Br / Br
                PortDescr: <model-name> - Gbic1000BaseT Port 1/28
                SysDescr : <model-name> (<release-number>)
                Address  : 10.13.13.47
-------------------------------------------------------------------------------

Total Neighbors : 1

-------------------------------------------------------------------------------
Capabilities Legend: (Supported/Enabled)
B= Bridge,    D= DOCSIS,    O= Other,     R= Repeater,
S= Station,   T= Telephone, W= WLAN,      r= Router
```

View the LLDP administrative status of all ports on the switch. You can also view this on a specific port.

```
Switch:1#show lldp port

======================================================================
                             LLDP Admin Port Status

======================================================================
----------------------------------------------------------------------
Port       AdminStatus  ConfigNotificationEnable  CdpAdminState
----------------------------------------------------------------------
1/1        txAndRx      disabled                  disabled
1/2        txAndRx      disabled                  disabled
1/3        txAndRx      disabled                  disabled
1/4        txAndRx      disabled                  disabled
...
...
```

View the LLDP reception statistics. You can also view this on a specific port.

```
Switch:1#show lldp rx-stats

=============================================================================
                                 LLDP Rx-Stats

=============================================================================

Port      Frames      Frames   Frames   TLVs        TLVs           AgeOuts
```

```
Num       Discarded   Errors   Total    Discarded   Unsupported
                                        (Non FA)    (Non FA)
-----------------------------------------------------------------------------
1/1       0           0        0        0           0              0
1/2       0           0        0        0           0              0
1/3       0           0        0        0           0              0
1/4       0           0        0        0           0              0
...
...
```

View the LLDP statistics:

```
Switch:1#show lldp stats

==============================================================
                                   LLDP Stats

==============================================================
Inserts    Deletes    Drops      Ageouts
--------------------------------------------------------------
4          0          0          0
--------------------------------------------------------------
```

View the LLDP transmission statistics:

```
Switch:1#show lldp tx-stats

======================================================================
                                 LLDP Tx-Stats

======================================================================

PORT NUM                 FRAMES
----------------------------------------------------------------------
1/1                      95
1/2                      95
1/3                      95
1/4                      95
1/5                      95
...
...
```

Variable definitions

Use the data in the following table to use the **`show lldp`** command.

Variable	Value
local-sys-data	Displays the LLDP local system data.
neighbor [port *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*]	Displays the LLDP neighbor system information. You can also view this on a specific port. Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).
port [*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*]	Displays the LLDP administrative status of a port or all ports on the switch.

Table continues…

Variable	Value
	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).
rx-stats [port *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*]	Displays the LLDP reception statistics on all ports on the switch, or on a specific port. Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).
stats	Displays the LLDP statistics.
tx-stats [port *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*]	Displays the LLDP transmission statistics on all ports on the switch or on a specific port. Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

Viewing LLDP neighbor information

Display information about LLDP neighbors to help you configure LLDP for maximum benefit.

About this task

Use this procedure to display LLDP neighbor information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To view LLDP neighbor information, enter:

   ```
   show lldp neighbor [port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]
   ```

Example

```
Switch:1#show lldp neighbor

================================================================================
                                 LLDP Neighbor
================================================================================

Port: 2/1       Index    : 1                  Time: 0 day(s), 00:19:59
                Protocol    : LLDP
                ChassisId: MAC Address        a4:25:1b:50:64:00
                PortId   : MAC Address        a4:25:1b:50:64:34
                SysName  : Switch1
                SysCap   : Br / Br
                PortDescr: 2/1
                Address  : 10.19.12.98
                SysDescr : <model-name> (<release-number>)  BoxType: <model-name>
--------------------------------------------------------------------------------
```

```
Total Neighbors : 1
--------------------------------------------------------------------------------
Capabilities Legend: (Supported/Enabled)
B= Bridge,    D= DOCSIS,    O= Other,     R= Repeater,
S= Station,   T= Telephone, W= WLAN,      r= Router
```

Variable definitions

Use the data in the following table to use the **`show lldp neighbor`** command.

Variable	Value
port *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*	Displays LLDP neighbor information on the specified port. Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port).

Viewing global LLDP statistics

Use this procedure to view and verify global LLDP statistics.

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. To view LLDP statistics, enter:

   `show lldp stats`

3. To view LLDP reception statistics, enter:

   `show lldp rx-stats`

4. To view LLDP transmission statistics, enter:

   `show lldp tx-stats`

5. **(Optional)** Clear global LLDP statistics:

   `clear lldp stats summary`

Example

View LLDP statistics:

```
Switch:1>enable
Switch:1#show lldp stats

=================================================================
                                   LLDP Stats
=================================================================
Inserts    Deletes    Drops      Ageouts
-----------------------------------------------------------------
0          0          0          0
-----------------------------------------------------------------
```

View LLDP transmission statistics:

```
Switch:1#show lldp tx-stats
================================================================
                                 LLDP Tx-Stats
================================================================

PORT NUM                 FRAMES
----------------------------------------------------------------
1/2                      100
```

View LLDP reception statistics:

```
Switch:1#show lldp rx-stats

================================================================
                                 LLDP Rx-Stats
=================================================================

Port  Frames      Frames   Frames   TLVs        TLVs         AgeOuts
Num   Discarded   Errors   Total    Discarded   Unrecognized
------------------------------------------------------------------
1/2   0           0        46       0           0            0
```

Viewing port-based LLDP statistics

Use this procedure to verify port-based LLDP statistics.

About this task

LLDP operates at the interface level. Enabling FA on a port automatically enables LLDP transmission and reception on the port. It also enables traffic tagging and disables spanning tree on that port.

Enabling FA on an MLT enables LLDP transmission and reception on *all* ports in the MLT.

Note:

When FA is enabled on ports in an MLT or LACP MLT, tagging is enabled and spanning tree is disabled on those ports.

When a port is removed from an MLT, LLDP transmission on that port stops and spanning tree is enabled. Any I-SID-to-VLAN mappings on that port are removed, if not already learned on any other port in the MLT. This also causes the Switched UNI I-SID to be deleted from the MLT. If however, the mappings are learned on another port on the MLT, then the Switched UNI I-SID continues to exist for that MLT.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To verify successful LLDP transmission on a port, enter:

   ```
   show lldp tx-stats port {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
   ```

3. To verify that a port receives LLDP PDUs successfully, enter:

`show lldp rx-stats port` *`{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`*

4. **(Optional)** To clear LLDP statistics on a port, or ports, enter:

   `clear lldp stats` *`{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`*

Example

Verify LLDP transmission statistics on a port:

```
Switch:1>en
Switch:1#show lldp tx-stats port 1/2
=================================================================
                                 LLDP Tx-Stats
=================================================================

PORT NUM                 FRAMES
-----------------------------------------------------------------
1/2                      100
```

Verify that the port is receiving LLDP PDUs:

```
Switch:1#show lldp rx-stats port 1/2

=================================================================================
                                 LLDP Rx-Stats
=================================================================================

Port      Frames      Frames   Frames   TLVs        TLVs           AgeOuts
Num       Discarded   Errors   Total    Discarded   Unsupported
                                         (Non FA)    (Non FA)
---------------------------------------------------------------------------------
1/2       0           0        46       0           0              0
```

Link Layer Discovery Protocol configuration using EDM

This section describes how to configure LLDP on your switch using EDM.

Configuring LLDP global information

Use this procedure to configure or view LLDP global information.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** > **802_1ab.LLDP** folders.
2. In the content pane, click the **Globals** tab.
3. After you make the required configuration changes, click **Apply** to save changes.

Globals field descriptions

Use the data in the following table to use the **Globals** tab.

Field	Description
lldpMessageTxInterval	Specifies the interval at which LLDP messages are transmitted. The default is 30 seconds.
lldpMessageTxHoldMultiplier	Specifies the multiplier used to calculate the time-to-live (TTL) value of an LLDP message. The default value is 4 seconds.
lldpReinitDelay	Specifies the delay in seconds between the time a port is disabled and the time it is re-initialized. The default is 1 second.
lldpTxDelay	Specifies the delay in seconds between successive LLDP transmissions. The default is 1 second. The recommended value is as follows: 1 < **lldpTxDelay** < (0.25 x **lldpMessageTxInterval**)
lldpNotificationInterval	Specifies the time interval between successive LLDP notifications. It controls the transmission of notifications. The default is 5 seconds.
Stats	
RemTablesLastChangeTime	Specifies the timestamp of LLDP missed notification events on a port, for example, due to transmission loss.
RemTablesInserts	Specifies the number of times the information advertised by a MAC Service Access Point (MSAP) is inserted into the respective tables.
RemTablesDeletes	Specifies the number of times the information advertised by an MSAP is deleted from the respective tables.
RemTablesDrops	Specifies the number of times the information advertised by an MSAP was not entered into the respective tables.
RemTablesAgeouts	Specifies the number of times the information advertised by an MSAP was deleted from the respective tables.

Viewing the LLDP port information

Use this procedure to view the LLDP port information.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** > **802_1ab.LLDP** folders.
2. In the content pane, click the **Port** tab.
3. View the administrative status of the port in the **AdminStatus** field. To modify, double-click on a cell and select a value from the drop-down list.
4. View whether the port is enabled for notifications in the **NotificationEnable** field. To modify, double-click on a cell and select a value from the drop-down list.

5. View the set of TLVs whose transmission using LLDP is always allowed by network management in the **TLVsTxEnable** field.
6. **(Optional)** Modify the TLVs as follows:
    a. To enable a TLV, select the appropriate check box, and click **Ok**. You can select more than one check box.
    b. To enable all TLVs, click **Select All**, and click **Ok**.
    c. To disable all TLVs, click **Disable All**, and click **Ok**.
7. View the CDP administrative status in the **CdpAdminState** field. To modify, double-click on a cell and select a value from the drop-down list.
8. Click **Apply** to save any configuration changes.
9. Click **Refresh** to verify the configuration.

LLDP Port information field descriptions

Use the data in the following table to use the **Port** tab.

Name	Description
PortNum	Specifies the port number.
AdminStatus	Specifies the administrative status of the port. The default is disabled.
NotificationEnable	Specifies whether the port is enabled or disabled for notifications. The default is disable (false).
TLVsTxEnable	Specifies the set of TLVs whose transmission using LLDP is always allowed by network management.

Viewing LLDP transmission statistics

Use this procedure to view the LLDP transmission statistics. You can also view the statistics graphically.

About this task

LLDP operates at the port interface level. Enabling FA on a port automatically enables LLDP transmission and reception on that port. It also enables traffic tagging and disables spanning tree on that port.

Enabling FA on an MLT enables LLDP transmission and reception on *all* ports in that MLT.

Note:

When a port is removed from an MLT, LLDP transmission on that port stops and spanning tree is enabled. Any I-SID-to-VLAN mappings on that port are removed, if not already learned on any other port in the MLT. This also causes the Switched UNI I-SID to be deleted from the MLT. If however, the mappings are learned on another port on the MLT, then the Switched UNI I-SID continues to exist for that MLT.

For ports in an LACP MLT, when FA is enabled, tagging is enabled on all ports in the LACP MLT. The consistency check for FA is based on key membership. If all ports with the same key do not support FA, FA is not successfully enabled on those ports.

Note:

If a slot is removed from the switch chassis, the statistics are not displayed on the slot ports. When the slot is inserted back again, the statistics counters are reset.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** > **802_1ab.LLDP** folders.
2. In the content pane, click the **TX Stats** tab.

   The transmission statistics are displayed.
3. To view the transmission statistics graphically for a port:
   1. In the content pane (on the right-hand-side), select a row and click the **Graph** button.

      The **TX Stats-Graph,<port-number>** tab displays.

      You can view a graphical representation of the LLDP frames transmitted (**FramesTotal**), for the following parameters:

      - AbsoluteValue
      - Cumulative
      - Average/sec
      - Minimum/sec
      - Maximum/sec
      - LastVal/sec
   2. To view the graph, select one of the above parameters and click the appropriate icon on the top left-hand-side of the menu bar to draw a line chart, area chart, bar chart or a pie chart.
   3. Click **Clear Counters** to clear the existing counters, and fix a reference point in time to restart the counters.
   4. Click **Export**, to export the statistical data to a file.
   5. To fix a poll interval, select an appropriate value from the **Poll Interval** drop-down list.

TX Stats field descriptions

Use the data in the following table to view the LLDP transmission statistics.

Field descriptions for the **TX Stats** tab.

Name	Description
PortNum	Specifies the port number.
FramesTotal	Specifies the total number of LLDP frames transmitted.

Field descriptions for the **TX Stats-Graph, <port-number>** tab.

Name	Description
AbsoluteValue	Specifies the absolute number of LLDP frames at a given point in time.
Cumulative	Specifies the cumulative rate of change of LLDP frames transmitted.
Average/sec	Specifies the average rate of change of LLDP frames transmitted.
Minimum/sec	Specifies the minimum rate of change of LLDP frames transmitted.
Maximum/sec	Specifies the maximum rate of change of LLDP frames transmitted.
LastVal/sec	Specifies the rate of change of LLDP frames transmitted in the last second.

Viewing LLDP reception statistics

Use this procedure to view the LLDP reception statistics. You can also view these statistics graphically.

About this task

LLDP operates at the port interface level. Enabling FA on a port automatically enables LLDP transmission and reception on that port. It also enables traffic tagging and disables spanning tree on that port.

Enabling FA on an MLT enables LLDP transmission and reception on *all* ports in that MLT.

Note:

When a port is removed from an MLT, LLDP transmission on that port stops and spanning tree is enabled. Any I-SID-to-VLAN mappings on that port are removed, if not already learned on any other port in the MLT. This also causes the Switched UNI I-SID to be deleted from the MLT. If however, the mappings are learned on another port on the MLT, then the Switched UNI I-SID continues to exist for that MLT.

For ports in an LACP MLT, when FA is enabled, tagging is enabled on all ports in the LACP MLT. The consistency check for FA is based on key membership. If all ports with the same key do not support FA, FA is not successfully enabled on those ports.

Note:

If a slot is removed from the switch chassis, the statistics are not displayed on the slot ports. When the slot is inserted back again, the statistics counters are reset.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** > **802_1ab.LLDP** folders.
2. In the content pane, click the **RX Stats** tab.

3. To view the reception statistics graphically for a port:

    a. Select a row and click **Graph**.

    The **RX Stats-Graph,<port-number>** tab displays.

    You can view a graphical representation of the following data:

    - **FramesDiscardedTotal** — Total number of LLDP received frames that were discarded.
    - **FramesErrors** — Total number of erroneous LLDP frames received.
    - **FramesTotal** — Total number of frames received.
    - **TLVsDiscardedTotal** — Total number of received TLVs that were discarded.
    - **TLVsUnrecognizedTotal** — Total number of unrecognized TLVs received.

    b. Select one of the above parameters and click the appropriate icon on the top left-hand-side corner of the menu bar to draw a line chart, area chart, bar chart or a pie chart.

    c. Click **Clear Counters** to clear the existing counters, and fix a reference point in time to restart the counters.

    d. Click **Export**, to export the statistical data to a file.

    e. To fix a poll interval, select an appropriate value from the **Poll Interval** drop-down list.

RX Stats field descriptions

Use the data in the following table to view the LLDP reception statistics.

Name	Description
PortNum	Specifies the port number.
FramesDiscardedTotal	Specifies the number of LLDP frames received on the port, but discarded, for any reason. This counter provides an indication of possible LLDP header formatting problems in the sending system, or LLDP PDU validation problems in the receiving system.
FramesErrors	Specifies the number of invalid LLDP frames received on the port.
FramesTotal	Specifies the total number of LLDP frames received on the port.
TLVsDiscardedTotal	Specifies the number of LLDP TLVs discarded on the port, for any reason.
TLVsUnrecognizedTotal	Specifies the number of LLDP TLVs on the port, that are unrecognized on that port. An unrecognized TLV is referred to as the TLV whose type value is in the range of reserved TLV types (000 1001–111 1110). An unrecognized TLV could be, for example, a basic management TLV from a later LLDP version.
AgeoutsTotal	Specifies the number of LLDP age-outs that occur on a specific port. An age-out is the number of times the complete set of information advertised by a particular MSAP is deleted, because the information timeliness interval has expired.

Field descriptions for the **RX Stats-Graph, <port-number>** tab.

Name	Description
AbsoluteValue	Specifies the absolute number of LLDP frames at a given point in time.
Cumulative	Specifies the cumulative rate of change of LLDP frames received.
Average/sec	Specifies the average rate of change of LLDP frames received.
Minimum/sec	Specifies the minimum rate of change of LLDP frames received.
Maximum/sec	Specifies the maximum rate of change of LLDP frames received.
LastVal/sec	Specifies the rate of change of LLDP frames received in the last second.

Viewing LLDP local system information

Use this procedure to view the LLDP local system information.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** > **802_1ab.LLDP** folders.
2. In the content pane, click the **Local System** tab.

Local System field descriptions

Use the data in the following table to use the **Local System** tab.

Name	Description
ChassisIdSubType	Indicates the encoding used to identify the local system chassis. • chassisComponent • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • local
ChassisId	Indicates the chassis ID of the local system.
SysName	Indicates local system name.
SysDesc	Indicates local system description.
SysCapSupported	Indicates the system capabilities supported on the local system.
SysCapEnabled	Indicates the system capabilities that are enabled on the local system.

Viewing LLDP local port information

Use this procedure to view the LLDP local port information.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** > **802_1ab.LLDP** folders.
2. In the content pane, click the **Local Port** tab.

Local port field descriptions

Use the data in the following table to use the **Local Port** tab.

Name	Description
PortNum	Indicates the port number.
PortIdSubType	Indicates the type of port identifier. • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • agentCircuitId • local
PortId	Indicates the identifier associated with the port, on the local system.
PortDesc	Indicates the description of the port, on the local system.

Viewing LLDP neighbor information

Use this procedure to view the LLDP neighbor information.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** > **Diagnostics** > **802_1ab.LLDP** folders.
2. In the content pane, click the **Neighbor** tab.

Neighbor field descriptions

Use the data in the following table to use the **Neighbor** tab.

Name	Description
TimeMark	Indicates the time filter. For more information about TimeFilter, see the TimeFilter textual convention in IETF RFC 2021.
LocalPortNum	Identifies the port on which the remote system information is received.
Index	Indicates a particular connection instance that is unique to the remote system.

Table continues…

Name	Description
ChassisIdSubtype	Indicates the type of encoding used to identify the remote system chassis. • chassisComponent • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • local
ChassisId	Indicates the chassis ID of the remote system.
SysCapSupported	Identifies the system capabilities supported on the remote system.
SysCapEnabled	Identifies the system capabilities enabled on the remote system.
SysName	Indicates the name of the remote system.
SysDesc	Indicates the description of the remote system.
PortIdSubType	Indicates the type of encoding used to identify the remote port.
PortId	Indicates the remote port ID.
PortDesc	Indicates the remote port description.
ProtocolType	Indicates whether the entry protocol is CDP or LLDP.
IpAddress	Indicates the neighbor’s IP address.

SMTP for email notification

Use the information in the following sections to understand email notification and its configuration using the CLI or the EDM.

Email notification

The switch can send email notification for failed components or other critical log-event conditions. The switch can also send periodic health status notifications.

Enable and configure a Simple Mail Transfer Protocol (SMTP) client on the switch for one SMTP server by specifying the server hostname or IPv4 address. To use a hostname, you must also configure a Domain Name System (DNS) client on the switch.

You must configure at least one email recipient and can create a maximum of five email recipients.

The switch can periodically send general health status notifications. Status email messages include information about the following items:

- General switch
- Chassis
- Card
- Temperature
- Power supplies
- Fans
- LEDs
- System errors
- Port lock
- Message control
- Operational configuration changes
- Current Uboot
- Port interfaces
- Port statistics

The switch maintains a default list of event IDs for which it generates an email notification. You can add specific event IDs to this list. To see the default list of event IDs, run the **show smtp event-id** command.

The following example shows an email that the switch sends for log events.

```
Subject: Logs from LabSwitch - 50712100008
From: <LabSwitch@default.com>
To: <test1@default.com>
CP1  [08/04/15 21:48:04.527:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR GlobalRouter
SNMP INFO 2k card up(CardNum=1 AdminStatus=1 OperStatus=1)
CP1  [08/04/15 21:48:04.527:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR GlobalRouter
SNMP INFO 2k card up(CardNum=1 AdminStatus=1 OperStatus=1)
CP1  [08/04/15 21:48:04.527:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR GlobalRouter
SNMP INFO 2k card up(CardNum=2 AdminStatus=1 OperStatus=1)
CP1  [08/04/15 21:50:03.511:UTC] 0x00088524 00000000 GlobalRouter SW INFO Boot sequence
successful
```

If you enable the SMTP client but the switch cannot reach the SMTP server, the switch generates an alarm. The switch holds log and status information in a queue until the connection with the SMTP server is restored. The message queue holds a maximum of 2,000 messages. If the queue fills, the switch drops new messages.

The following text is an example of the alarm that the switch generates when it cannot connect to the SMTP server.

```
CP1  [06/10/15 19:27:07.901:EST] 0x00398600 0e600000 DYNAMIC SET GlobalRouter SMTP
WARNING SMTP: Unable to establish connection with server: mailhost.usae.company.com, port:
25
```

If the switch cannot establish a connection to the SMTP server, verify that the server IP address or hostname, and the TCP port are correct. If you specify the server hostname, confirm that the IP address for the DNS server is correct. Check for network issues such as unplugged cables.

If the SMTP server rejects the email message, the switch generates a log message.

Configuring email notification

Configure the SMTP feature to generate email notifications for component failures, critical conditions, or general system health status.

About this task

The SMTP feature is disabled by default.

Before you begin

- To identify the SMTP server by hostname, you must first configure a DNS client on the switch. For more information about how to configure a DNS client, see *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the TCP port the client uses to open a connection with the SMTP server:

   ```
   smtp port <1-65535>
   ```

   Note:

   The port you specify must match the port that the SMTP server uses.

3. Configure email recipients:

   ```
   smtp receiver-email add WORD<3-1274>
   ```

   ```
   smtp receiver-email remove WORD<3-1274>
   ```

   Note:

   You must configure at least one recipient.

4. Configure the SMTP server hostname or IPv4 address:

   ```
   smtp server WORD<1-256>
   ```

5. **(Optional)** Configure a sender email address:

   ```
   smtp sender-email WORD<3-254>
   ```

6. **(Optional)** Add or remove log events to the default list that generate email notification:

   ```
   smtp event-id add WORD<1-1100>
   ```

    `smtp event-id remove` *`WORD<1-1100>`*

7. **(Optional)** Configure the status update interval:

   `smtp status-send-timer` *`<0 | 30-43200>`*

8. Enable the SMTP client:

   `smtp enable`

9. Configure an SMTP domain name:

   `smtp domain-name` *`WORD<1-254>`*

10. Verify the configuration:

    `show smtp [event-id]`

Example

Configure the SMTP client to use TCP port 26 to communicate with an SMTP server that is using port 26. Add two receiver email addresses, configure the server information using an IPv4 address, and enable the SMTP feature. Finally, configure an SMTP domain name, and then verify the configuration.

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#smtp port 26
Switch:1(config)#smtp receiver-email add test1@default.com,test2@default.com
Switch:1(config)#smtp server 192.0.2.1
Switch:1(config)#smtp enable
Switch:1(config)#smtp domain-name test mailer
Switch:1(config)#show smtp
================================================================================
                                SMTP Information
================================================================================
        SMTP Status:  Enabled
     Server Address:  192.0.2.1
        Server Port:  26
  Status send Timer:  30 (seconds)
       Sender Email:  LabSwitch@default.com
        Domain Name:  test mailer
    Receiver Emails:  test1@default.com
                      test2@default.com
```

Add an event ID to the list for which the switch sends email notification on a log event. Verify the configuration.

```
Switch:1(config)#smtp event-id add 0x0000c5ec
Switch:1(config)#show smtp event-id
================================================================================
                           SMTP Event IDs Information
================================================================================
Log Event IDs: (total: 51)
           0x000045e3,0x00004602,0x00004603,0x0000c5ec,0x000106ce,0x000106cf
           0x000106d0,0x000106d1,0x000106d2,0x000106d4,0x000106d8,0x000106d9
           0x000106da,0x000106f8,0x000106f9,0x000106fb,0x00010775,0x00010776
           0x000107f5,0x000107f6,0x000305c8,0x000305ca,0x000305f1,0x00030637
           0x00040506,0x00040507,0x00040508,0x00040509,0x000646da,0x000646db
           0x00088524,0x000d8580,0x000d8586,0x000d8589,0x000e4600,0x000e4601
           0x000e4602,0x000e4603,0x000e4604,0x000e4605,0x000e4606,0x000e4607
```

```
              0x000e4608,0x000e4609,0x001985a0,0x00210587,0x00210588,0x00210595
              0x00210596,0x0027458a,0x0027458d

Default Event IDs: (total: 50)
              0x000045e3,0x00004602,0x00004603,0x000106ce,0x000106cf,0x000106d0
              0x000106d1,0x000106d2,0x000106d4,0x000106d8,0x000106d9,0x000106da
              0x000106f8,0x000106f9,0x000106fb,0x00010775,0x00010776,0x000107f5
              0x000107f6,0x000305c8,0x000305ca,0x000305f1,0x00030637,0x00040506
              0x00040507,0x00040508,0x00040509,0x000646da,0x000646db,0x00088524
              0x000d8580,0x000d8586,0x000d8589,0x000e4600,0x000e4601,0x000e4602
              0x000e4603,0x000e4604,0x000e4605,0x000e4606,0x000e4607,0x000e4608

              0x000e4609,0x001985a0,0x00210587,0x00210588,0x00210595,0x00210596
              0x0027458a,0x0027458d

Remove From Default: (total: 0)

Add List: (total: 1)
              0x0000c5ec
```

Variable definitions

Use the data in the following table to use the **smtp port** command.

Variable	Value
<1–65535>	Specifies the TCP port on the switch that the SMTP client uses to communicate with the SMTP server. The default value is 25. **Note:** You must disable the SMTP feature before you can change an existing SMTP port configuration. The port you specify must match the port that the SMTP server uses.

Use the data in the following table to use the **smtp receiver-email** command.

Variable	Value
add *WORD<3-1274>*	Adds an email address to the recipient list. The recipients receive the email notification generated by the switch. You must configure at least one email recipient and can create a maximum of five email recipients. You can specify multiple addresses in a single command by separating them with a comma. You cannot use quotation marks (“) or commas (,) in email addresses. Other restrictions for the format of the email address follow RFC 5321. The maximum length for the address is 254 characters.

Table continues…

Variable	Value
remove *WORD<3-1274>*	Removes an email address from the recipient list. The recipients receive the email notification generated by the switch. You can specify multiple addresses in a single command by separating them with a comma. You cannot use quotation marks (") or commas (,) in email addresses. Other restrictions for the format of the email address follow RFC 5321. The maximum length for the address is 254 characters.

Use the data in the following table to use the **`smtp server`** command.

Variable	Value
WORD<1-256>	Specifies the SMTP server address. You can use either a hostname or IPv4 address. If you use a hostname, you must configure the DNS client on the switch.

Use the data in the following table to use the **`smtp sender-email`** command.

Variable	Value
WORD<3-254>	Specifies the email address that appears in the From field of the message that the switch generates. By default, the switch uses *<SystemName>*@default.com.

Use the data in the following table to use the **`smtp event-id`** command.

Variable	Value
add *WORD<1-1100>*	Adds a log event to the list of events that generate email notification. You can specify multiple event IDs in a single command by separating them with a comma. The event ID can be up to 10 digits in hexadecimal format.
remove *WORD<1-1100>*	Removes a log event from the list of events that generate email notification. You can specify multiple event IDs in a single command by separating them with a comma. The event ID can be up to 10 digits in hexadecimal format.

Use the data in the following table to use the **`smtp status-send-timer`** command.

Variable	Value
<0 | 30-43200>	Specifies the interval, in seconds, at which the switch sends status information. The default is 30 seconds. A value of 0 means the switch does not send status information.

Use the data in the following table to use the **`smtp domain-name`** command.

Variable	Value
WORD<1-254>	Specifies the SMTP host name or IPv4 address (string length 1–254).

Use the data in the following table to use the **`show smtp`** command.

Variable	Value
event-id	Shows a list of active event IDs for which the switch generates email notification. The command output includes the default list of IDs and IDs you specifically add or remove.

Configuring email notification

Configure the SMTP feature to generate email notifications for component failures, critical conditions, or general system health status.

About this task

The SMTP feature is disabled by default.

Before you begin

- To identify the SMTP server by hostname, you must first configure a DNS client on the switch. For more information about how to configure a DNS client, see *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.
2. Click **SMTP**.
3. Click the **Globals** tab.
4. In the **ServerAddress** field, configure the SMTP server address.
5. In the **ReceiverEmailsList** field, add email recipients.

   Note:

   You must configure at least one recipient.
6. **(Optional)** In the **SenderEmail** field, configure a sender email address to use an address other than the default.

7. In the **DomainName** field, configure an SMTP domain name.
8. In the **Port** field, configure the TCP port that the client uses to open a connection with the SMTP server.
9. **(Optional)** In the **SystemStatusSendTimer** field, configure the status update interval.
10. Click **enable** to enable the SMTP client.
11. **(Optional)** In the **LogEventIds** field, add or remove log events to the default list that generates an email notification.
12. Click **Apply**.

Globals field descriptions

Use the data in the following table to use the Globals tab.

Name	Description
ServerAddressType	Specifies the type of server address as either an IPv4 address or a hostname. If you use a hostname, you must configure the DNS client on the switch.
ServerAddress	Specifies the SMTP server address. You can use either a hostname or an IPv4 address. If you use a hostname, you must configure the DNS client on the switch.
ReceiverEmailsList	Specifies the recipient list. The recipients receive the email notification generated by the switch. You must configure at least one email recipient and can create a maximum of five email recipients. You can specify multiple addresses in a single command by separating them with a comma. You cannot use quotation marks (“) or commas (,) in email addresses. Other restrictions for the format of the email address follow RFC5321. The maximum length for the address is 254 characters.
NumOfEmails	Shows the total number of addresses in **ReceiverEmailsList**.
SenderEmail	Specifies the email address that appears in the From field of the message that the switch generates. By default, the switch uses *SystemName*@default.com.
DomainName	Specifies the SMTP domain name. The maximum length is 254 characters.
Port	Specifies the TCP port on the switch that the SMTP client uses to communicate with the SMTP server. The default value is 25.

Table continues…

Name	Description
	✱ **Note:** You must disable the SMTP feature before you can change an existing SMTP port configuration. The port you specify must match the port that the SMTP server uses.
SystemStatusSendTimer	Specifies the interval, in seconds, at which the switch sends status information. The default is 30 seconds. A value of 0 means the switch does not send status information.
Enable	Enables or disables the SMTP feature. By default, SMTP is disabled.
LogEventIds	Specifies the list of events that generate email notification. You can specify multiple event IDs in a single command by separating them with a comma. The event ID can be up to 10 digits in hexadecimal format.
NumOfEventIds	Shows the total number of IDs in **LogEventIds**.
DefaultLogEventIds	Shows the default list of event IDs that generate email notification.
NumOfDefaultEventIds	Shows the total number of IDs in **DefaultLogEventIds**.

Support for 100 Gbps Ethernet

Use the information in the following sections to understand the documentation updates in support of the 100 Gbps Ethernet.

100 GbE port considerations

Clause 91 Forward Error Correction (FEC) is mandatory for ports with 100GbSR4 and 100GbCR4 modules plugged in. No separate configuration parameter exists for Clause 91 FEC. The system automatically enables Clause 91 FEC upon detection of these two modules. However, auto-negotiation should be enabled for this to take effect. Ensure that you enable auto-negotiation for ports with 100GbSR4 or 100GbCR4 modules plugged in.

Although auto-negotiation is mandatory as per the 100GbCR4 standard, and this is the default software configuration, you can disable auto-negotiation to connect with older systems that do not support it. The system does not support Clause 91 FEC on 100GbCR4 links with auto-negotiation disabled.

Clause 91 FEC does not apply when the 100 GbE ports are channelized.

Port-based shaping

Configuring the port-based shaper

Use port-based shaping to rate-limit all outgoing traffic to a specific rate.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   
   configure terminal
   ```

2. Configure port-based shaping for a 10 Gbps port:

   ```
   qos if-shaper [port {slot/port[/sub-port]}] shape-rate
   <1000-10000000>
   ```

3. Configure port-based shaping for a 40 Gbps port:

   ```
   qos if-shaper [port {slot/port[/sub-port]}] shape-rate
   <1000-40000000>
   ```

4. Configure port-based shaping for a 100 Gbps port:

   ```
   qos if-shaper [port {slot/port[/sub-port]}] shape-rate
   <1000-100000000>
   ```

OSPF default cost for 100 Gbps Ethernet

Configuring OSPF globally

Configure OSPF parameters on the switch so that you can control OSPF behavior on the system. The switch uses global parameters to communicate with other OSPF routers. Globally configure OSPF before you configure OSPF for an interface, port, or VLAN.

Before you begin

- Ensure that the switch has an IP interface.
- You configure OSPF on a VRF instance the same way you configure the GlobalRouter, except that you must use VRF Router Configuration mode and the prefix **`ip ospf`** to commands. Not all parameters are configurable on non0 VRFs.

Procedure

1. Enter OSPF Router Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

```
router ospf
```

2. Configure the OSPF router ID:

   ```
   router-id {A.B.C.D}
   ```

3. Configure the router as an autonomous system boundary router (ASBR):

   ```
   as-boundary-router enable
   ```

   Note:

   Configure the following steps as and when needed.

4. Enable the automatic creation of OSPF virtual links:

   ```
   auto-vlink
   ```

5. Configure the OSPF default metrics:

   ```
   default-cost {ethernet|fast-ethernet|forty-gig-ethernet|gig-
   ethernet|hundred-gig-ethernet|ten-gig-ethernet|twentyfive-gig-
   ethernet} <1-65535>]
   ```

   ```
   default-cost vlan <1-65535>]
   ```

   Note:

   Different hardware platforms support different port speeds. For more information, see your hardware documentation.

6. Configure the OSPF hold-down timer value:

   ```
   timers basic holddown <3-60>
   ```

7. Enable the RFC1583 compatibility mode:

   ```
   rfc1583-compatibility enable
   ```

8. Enable the router to issue OSPF traps:

   ```
   trap enable
   ```

9. Verify the OSPF configuration:

   ```
   show ip ospf [vrf WORD<1-16>] [vrfids WORD<0-512>]
   ```

10. Exit OSPF Router Configuration mode:

    ```
    exit
    ```

    You return to Global Configuration mode.

11. Enable OSPF for the switch:

    ```
    router ospf enable
    ```

Example

Configure the OSPF router ID to 192.0.2.2, enable the automatic creation of OSPF virtual links, and enable traps. Configure the default cost metric for Ethernet to 101, for fast Ethernet to 110, and for gig-Ethernet, ten-gig-Ethernet, twentyfive-gig-ethernet, forty-gig-Ethernet, and hundred-gig-ethernet to 20, and vlan to 1. Configure the basic holdown to 10. Enable OSPF for the switch, and review the configuration.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#router ospf
Switch:1(config-ospf)#router-id 192.0.2.2
Switch:1(config-ospf)#auto-vlink
Switch:1(config-ospf)#default-cost ethernet 101
Switch:1(config-ospf)#default-cost fast-ethernet 110
Switch:1(config-ospf)#default-cost gig-ethernet 20
Switch:1(config-ospf)#default-cost ten-gig-ethernet 20
Switch:1(config-ospf)#default-cost twentyfive-gig-ethernet 20
Switch:1(config-ospf)#default-cost Forty-gig-ethernet 20
Switch:1(config-ospf)#default-cost hundred-gig-ethernet 20
Switch:1(config-ospf)#default-cost vlan 2
Switch:1(config-ospf)#timers basic holddown 10
Switch:1(config-ospf)#trap enable
Switch:1(config-ospf)#exit
Switch:1(config)#router ospf enable
Switch:1(config)#show ip ospf

================================================================================
                          OSPF General - GlobalRouter
================================================================================

            RouterId: 1.1.1.1
           AdminStat: disabled
       VersionNumber: 2
    AreaBdrRtrStatus: false
      ASBdrRtrStatus: true
      Bad-Lsa-Ignore: false
      ExternLsaCount: 0
   ExternLsaCksumSum: 0(0x0)
          TOSSupport: 0
    OriginateNewLsas: 0
           RxNewLsas: 0
          TrapEnable: false
  AutoVirtLinkEnable: false
     SpfHoldDownTime: 10
Rfc1583Compatibility: disable
         Helper mode: enabled

default-metric :
                         ethernet - 101
                    fast-ethernet - 110
                     gig-ethernet - 20
                 ten-gig-ethernet - 20
          twentyfive-gig-ethernet - 20
               forty-gig-ethernet - 20
             hundred-gig-ethernet - 20
                                               Vlan - 1
```

Configuring OSPF globally

Configure OSPF parameters, such as automatic virtual links and OSPF metrics, so you can control OSPF behavior on the system.

Before you begin

- Change the VRF instance as required to configure OSPF on a specific VRF instance. The VRF must have an RP trigger of OSPF. Not all parameters are configurable on non0 VRFs.
- Assign an IP address to the switch.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **IP**.
2. Click **OSPF**.
3. Click the **General** tab.
4. Specify the OSPF router ID.
5. In AdminStart, select **enabled**.
6. **(Optional)** If required, configure the metrics that OSPF uses for different link speeds.

   The lower the metric, the more likely that OSPF chooses the link to route an OSPF packet.

   Note:

   Different hardware platforms support different port speeds. For more information, see your hardware documentation.
7. **(Optional)** To enable the switch to use OSPF SNMP traps, select the **TrapEnable** check box.
8. **(Optional)** To enable the automatic creation of virtual links, select the **AutoVirtLinkEnable** check box.
9. **(Optional)** Configure the OSPF holddown timer as required.
10. Click **Apply**.

General field descriptions

Use the data in the following table to use the **General** tab.

Note:

Different hardware platforms support different port speeds. For more information, see your hardware documentation.

Name	Description
RouterId	Specifies the OSPF router ID. This variable has the same format as an IP address but distinguishes this router from other routers in the OSPF domain.
AdminStat	Shows the administrative status of OSPF for the router. Enabled denotes that the OSPF process is active on at least one interface; disabled disables it for all interfaces. The default is disabled.
VersionNumber	Specifies the OSPF version.
AreaBdrRtrStatus	Denotes if this router is an area border router (ABR).

Table continues…

Name	Description
	AreaBdrRtrStatus value must be true to create a virtual router interface.
ASBdrRtrStatus	Specifies ASBR status. If you select the ASBdrRtrStatus check box, the router is an autonomous system boundary router (ASBR).
ExternLsaCount	Shows the number of external (LS type 5) link-state advertisements in the link-state database.
ExternLsaCksumSum	Shows the 32-bit unsigned sum of the link-state checksums of the external link-state advertisements in the link-state database. This sum determines if a change occurred in a router link-state database and compares the link-state databases of two routers.
OriginateNewLsas	Shows the number of new link-state advertisements originated from this router. This number increments each time the router originates a new link-state advertisement (LSA).
RxNewLsas	Shows the number of received link-state advertisements that are new instances. This number does not include new instances of self-originated link-state advertisements.
10MbpsPortDefaultMetric	Indicates the default cost applied to 10 Mbps interfaces (ports). The default is 100.
100MbpsPortDefaultMetric	Indicates the default cost applied to 100 Mbps interfaces (ports). The default is 10.
1000MbpsPortDefaultMetric	Indicates the default cost applied to 1 Gbps interfaces (ports). The default is 1.
10000MbpsPortDefaultMetric	Indicates the default cost applied to 10 Gbps interfaces (ports). The default is 1.
25000MbpsPortDefaultMetric	Indicates the default cost applied to 25 Gbps interfaces (channelized 100 Gbps ports). The default is 1.
40000MbpsPortDefaultMetric	Indicates the default cost applied to 40 Gbps interfaces (ports). The default is 1.
100000MbpsPortDefaultMetric	Indicates the default cost applied to 100 Gbps interfaces (ports). The default is 1.
VlanDefaultMetric	Configures the VLAN interfaces default metric. The default is 10.
TrapEnable	Indicates whether to enable traps for OSPF. The default is false.
AutoVirtLinkEnable	Enables or disables the automatic creation of virtual links. The default is false.
SpfHoldDownTime	Specifies the OSPF holddown timer (3–60 seconds). The default is 10 seconds. The holddown timer delays a metric change due to a routing table update by x seconds. If you configure the timer to 0, OSPF accepts a new metric change immediately.
OspfAction	Initiates a new Shortest Path First (SPF) run to update the routing table. The default is none.

Table continues…

Name	Description
Rfc1583Compatability	Controls the preference rules used when the router chooses among multiple autonomous system external (ASE) LSAs which advertise the same destination. If enabled, the preference rule is the same as that specified by RFC 1583. If disabled, the preference rule is as described in RFC 2328, which can prevent routing loops when ASE LSAs for the same destination originate from different areas. The default is disable.
LastSpfRun	Indicates the time since the last SPF calculation made by OSPF.
HelperModeDisable	Disables the helper mode. It is enabled by default.

Viewing the OSPF default cost information

View the OSPF default cost information to ensure accuracy.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the OSPF cost information:

   ```
   show ip ospf default—cost [vrf WORD<1-16>] [vrfids WORD<0-512>]
   ```

Example

Note:

Different hardware platforms support different port speeds. For more information, see your hardware documentation.

View the OSPF cost information on the switch:

```
Switch:1#show ip ospf default-cost vrf 3

=========================================================================================
                          OSPF Default Metric - VRF 3

=========================================================================================
    10MbpsPortDefaultMetric: 100
   100MbpsPortDefaultMetric: 10
  1000MbpsPortDefaultMetric: 1
 10000MbpsPortDefaultMetric: 1
25000MbpsPortDefaultMetric:  1
 40000MbpsPortDefaultMetric: 1
100000MbpsPortDefaultMetric: 1
```

Variable definitions

Use the data in the following table to use the **`show ip ospf default-cost`** command.

Variable	Value
vrf WORD<1-16>	Specifies a VRF by name.
vrfids WORD<0-512>	Specifies a range of VRF IDs.

Configuring OSPF default metrics

About this task

Use the following procedure to configure global OSPF default metrics.

Procedure

1. Enter OSPF Router Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   router ospf
   ```

2. Configure OSPF default-cost:

   ```
   ipv6 default-cost {ethernet|fast-ethernet|forty-gig-ethernet|
   hundred-gig-ethernet|gig-ethernet|ten-gig-ethernet|twentyfive-gig-
   ethernet|vlan} <1-65535>
   ```

   Note:

   Different hardware platforms support different port speeds. For more information, see your hardware documentation.

Example

Configure IPv6 default cost metric for Ethernet to 100, for fast Ethernet to 20, for gig-ethernet, twentyfive-gig-ethernet, forty-gig-Ethernet, and hundred-gig-ethernet to 2, and VLAN to 1.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#router ospf
Switch:1(config-ospf)#ipv6 default-cost ethernet 100
Switch:1(config-ospf)#ipv6 default-cost fast-ethernet 20
Switch:1(config-ospf)#ipv6 default-cost gig-ethernet 2
Switch:1(config-ospf)#ipv6 default-cost ten-gig-ethernet 2
Switch:1(config-ospf)#ipv6 default-cost Forty-gig-ethernet 2
Switch:1(config-ospf)#ipv6 default-cost twentyfive-gig-ethernet 2
Switch:1(config-ospf)#ipv6 default-cost hundred-gig-ethernet 2
Switch:1(config-ospf)#ipv6 default-cost vlan 1
```

Variable definitions

Use the data in the following table to use the **`ipv6 default-cost`** command.

Note:

Different hardware platforms support different port speeds. For more information, see your hardware documentation.

Variable	Value
ethernet *<1-65535>*	Configures the IPv6 OSPF default metrics. The lower the metric, the more likely that OSPF chooses the link to route an OSPF packet.

Table continues…

Variable	Value
	ethernet is for 10 Mb/s Ethernet (default is 100).
fast-ethernet <*1-65535*>	Configures the IPv6 OSPF default metrics. The lower the metric, the more likely that OSPF chooses the link to route an OSPF packet. fast-ethernet is for 100 Mb/s Fast-Ethernet (default is 100).
forty-gig-ethernet <*1-65535*>	Configures the IPv6 OSPF default metrics. The lower the metric, the more likely that OSPF chooses the link to route an OSPF packet. forty-gig-ethernet is for 10 Mb/s Forty-Gigabit-Ethernet (default is 1).
gigabit-ethernet <*1-65535*>	Configures the IPv6 OSPF default metrics. The lower the metric, the more likely that OSPF chooses the link to route an OSPF packet. gigabit-ethernet is for 10 Mb/s Gigabit-Ethernet (default is 1).
hundred-gig-ethernet <*1-65535*>	Configures the IPv6 OSPF default metrics. The lower the metric, the more likely that OSPF chooses the link to route an OSPF packet. hundred-gig-ethernet is for 100 Gigabit Ethernet (default is 1).
ten-gig-ethernet <1-65535>	Configures the IPv6 OSPF default metrics. The lower the metric, the more likely that OSPF chooses the link to route an OSPF packet. ten-gig-ethernet is for 10 Mb/s Ten-Gigabit-Ethernet (default is 1).
twentyfive-gig-ethernet <*1-65535*>	Configures the IPv6 OSPF default metrics. The lower the metric, the more likely that OSPF chooses the link to route an OSPF packet. On a channelized 100 Gbps port, the default-cost for each 25 Gbps channel is 1.
vlan <*1-65535*>	Configures the IPv6 OSPF default metrics. The lower the metric, the more likely that OSPF chooses the link to route an OSPF packet. vlan is for Vlan interfaces (default is 10).

Configuring global default metrics

Configure the metrics that OSPF uses for different link speeds. The lower the metric, the more likely that OSPF chooses the link to route an OSPF packet.

Note:

Different hardware platforms support different port speeds. For more information, see your hardware documentation.

Before you begin

- Change the VRF instance as required to configure OSPF on a specific VRF instance. The VRF must have an RP trigger of OSPF. Not all parameters are configurable on non0 VRFs.

Procedure

1. In the navigation tree, expand the **Configuration** > **IP** folders.
2. Click **OSPF**.
3. Click the **General** tab.
4. Change the metric for one or all of the following:
   - 10MbpsPortDefaultMetric
   - 100MbpsPortDefaultMetric
   - 1000MbpsPortDefaultMetric
   - 10000MbpsPortDefaultMetric
   - 25000MbpsPortDefaultMetric
   - 40000MbpsPortDefaultMetric
   - 100000MbpsPortDefaultMetric
5. Click **Apply**.

OSPFv3 default cost for 100 Gbps Ethernet

Configuring OSPF globally

Configure OSPFv3 globally to enable it on the system and to configure the router ID.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable OSPFv3 for IPv6:

   ```
   router ospf ipv6-enable
   ```

   The default is disabled.

3. Log on to OSPF Router Configuration mode:

   ```
   router ospf
   ```

4. Specify the router ID:

   ```
   ipv6 router-id {A.B.C.D}
   ```

5. Optionally, make the router an autonomous system (AS) boundary router (BR):

   ```
   ipv6 as-boundary-router enable
   ```

   Enable the ASBR if the router attaches at the edge of the OSPF network, and has one or more interfaces that run an interdomain routing protocol. The default is disabled.

Example

Enable OSPFv3 for IPv6:

```
Switch:1(config)#router ospf ipv6-enable
```

Log on to OSPF Router Configuration mode:

```
Switch:1(config)#router ospf
```

Specify the router ID:

```
Switch:1(config-ospf)#ipv6 router-id 1.1.1.1
```

Variable definitions

Use the data in the following table to use the **`ipv6 router-id`** command.

Variable	Value
{A.B.C.D}	Specifies a 32–bit integer that identifies the router in the autonomous system. This value must be unique. The default value will be one of the IPv4 interface addresses.

Viewing OSPFv3 default cost information

About this task

Use the following procedure to View the OSPF default cost information, to ensure accuracy.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the OSPF cost information:

   ```
   show ipv6 ospf default-cost
   ```

Example

```
Switch:1#show ipv6 ospf default-cost
==================================================================================
                            IPv6 OSPF Default Metric
==================================================================================
    10MbpsPortDefaultMetric: 100
   100MbpsPortDefaultMetric: 10
  1000MbpsPortDefaultMetric: 1
 10000MbpsPortDefaultMetric: 1
```

```
 25000MbpsPortDefaultMetric: 1
 40000MbpsPortDefaultMetric: 1
100000MbpsPortDefaultMetric: 1
          VlanDefaultMetric: 10
```

Support for 100 Gbps QSFP28 transceivers

The following sections detail the documentation updates in support of the introduction of the 100 Gbps QSFP28 transceivers.

Resetting a QSFP+ or QSFP28 transceiver

Reset a transceiver to simulate removal and reinsertion of the transceiver, which can be helpful in troubleshooting. For example, if authentication of the transceiver fails but you believe the transceiver is a qualified Avaya part, you can reset the transceiver to begin the authentication process again.

About this task

Resetting the transceiver stops traffic and triggers log messages similar to the removal and insertion of the transceiver.

Before you begin

- Before you use the **`pluggable-optical-module reset`** command, ensure the port is administratively down to avoid link flaps.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Reset the transceiver:

   `pluggable-optical-module reset` *`{slot/port[/sub-port]}`*

   Important:

   Not all hardware platforms support these port types. For more information, see your hardware documentation.

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#pluggable-optical-module reset 1/41
Switch:1(config)#
CP1 [06/25/14 22:15:09.644] 0x0000c5e7 00300001.232 DYNAMIC SET GlobalRouter HW INFO Link
Down(1/41)
CP1  [06/25/14 22:15:10.267] 0x000e0597 00000000 GlobalRouter HAL INFO GBIC removed from
slot 1 Port 41 Type:40GbSR4 Vendor:Avaya
CP1  [06/25/14 22:15:13.015] 0x000e0598 00000000 GlobalRouter HAL INFO GBIC inserted in
```

```
slot 1 Port 41 Type:40GbSR4 Vendor:Avaya
CP1 [06/25/14 22:15:14.562] 0x0000c5ec 00300001.232 DYNAMIC CLEAR GlobalRouter HW INFO
Link Up(1/41)
```

```
Switch:1(config)#pluggable-optical-module reset 1/1
Switch:1(config)#CP1  [03/31/16 10:48:24.492:UTC] 0x0000c5e7 00300001.384 DYNAMIC SET
GlobalRouter HW INFO Link Down(1/1)
CP1  [03/31/16 10:48:24.601:UTC] 0x000e0597 00000000 GlobalRouter HAL INFO GBIC removed
from slot 1 Port 1 Type:100GbCR4 Vendor:Avaya
CP1  [03/31/16 10:48:24.710:UTC] 0x0000c5e7 00300001.385 DYNAMIC SET GlobalRouter HW INFO
Link Down(1/2)
CP1  [03/31/16 10:48:26.668:UTC] 0x000e0598 00000000 GlobalRouter HAL INFO GBIC inserted
in slot 1 Port 1 Type:100GbCR4 Vendor:Avaya
CP1  [03/31/16 10:48:26.988:UTC] 0x0000c5ec 00300001.385 DYNAMIC CLEAR GlobalRouter HW
INFO Link Up(1/2)
CP1  [03/31/16 10:48:27.099:UTC] 0x0000c5ec 00300001.384 DYNAMIC CLEAR GlobalRouter HW
INFO Link Up(1/1)
```

Digital Diagnostic Monitoring

Use Digital Diagnostic Monitoring (DDM) to monitor laser operating characteristics such as temperature, voltage, current, and power. This feature works at any time during active laser operation without affecting data traffic.

The following optical transceivers support DDM:

- 1 Gbps Small Form Factor Pluggable (SFP)
- 10 Gbps Small Form Factor Pluggable plus (SFP+)
- 40 Gbps Quad Small Form Factor Pluggable plus (QSFP+)
- 100 Gbps Quad Small Form Factor Pluggable 28 (QSFP28)

Note:

Not all hardware platforms support each form factor. For more information on supported form factors, see your hardware documentation.

Digital Diagnostic Interface (DDI) is an interface that supports DDM. These devices provide real-time monitoring of individual DDI transceivers. The DDM software provides warnings or alarms after the temperature, voltage, laser bias current, transmitter power or receiver power fall outside of vendor-specified thresholds during initialization.

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

Chapter 4: Important notices

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

Hardware compatibility

VOSS 5.3 software is supported only on the VSP 8404C hardware platform. It is not supported on other hardware platforms.

Software scaling capabilities

This section lists the software scaling capabilities of the VSP 8404C and the existing VSP 8000 Series platforms.

Note:

Unless explicitly stated, the scaling capabilities listed are supported on all VSP 8000 Series platforms, including the VSP 8404C.

Table 5: Software scaling capabilities

	Maximum number supported on VSP 8000 Series
Layer 2	
Directed Broadcast interfaces	200*
Note: * The number of Directed Broadcast interfaces must be equal to, or less than, 200. However, if you configure VLANs with both **NLB** and **Directed Broadcast**, you can only scale up to 100 VLANs.	
MAC table size (with SPBM)	112,000
Port based VLANs	4,059
Private VLANs (E-Tree)	4,059
Protocol based VLANs (IPv6 only)	1

Table continues…

	Maximum number supported on VSP 8000 Series
RSTP instances	1
MSTP instances	12
LACP aggregators	84 (up to 96 with channelization)
Ports per LACP aggregator	8-active
MLT groups	84 (up to 96 with channelization)
Ports per MLT group	8
SLPP VLANs	128
VLACP interfaces	84 (up to 96 with channelization)
Microsoft NLB cluster IP interfaces	200*
Note: * The number of NLB cluster IP interfaces multiplied by the number of configured clusters must be less than or equal to 200. The number of NLB cluster IP interfaces is the key, not the number of VLANs. You can configure 1 VLAN with up to 200 NLB cluster IP interfaces or configure up to 200 VLANs with 1 NLB cluster IP interface per VLAN. For example: `1 NLB cluster IP interface x 200 clusters = 200` or `2 NLB cluster IP interfaces x 100 clusters = 200` However, if you configure VLANs with both **NLB** and **Directed Broadcast**, you can only scale up to 100 VLANs assuming there is only 1 NLB cluster IP interface per VLAN.	
Layer 3 (IPv4 & IPv6 Common)	
IP interfaces (IPv4 or IPv6)	506 *See note in the row below
VRRP interfaces (IPv4/IPv6)	252 *See note in the row below
Routed Split Multi-Link Trunking (RSMLT) interfaces (IPv4 or IPv6)	252 *See note in the row below
Note: * The number of IP interfaces plus the number of VRRP interfaces plus the number of RSMLT interfaces plus 2 (if IP shortcuts is enabled) should not exceed 508.	
VRRP interfaces with fast timers (200ms) - IPv4/IPv6	24
ECMP groups/paths per group	1,000/8
OSPF v2/v3 interfaces	500
OSPF v2/v3 neighbors (adjacencies)	500
OSPF areas	12 for each VRF 80 for the switch
DHCP Relay forwarding (IPv4 or IPv6)	1,024

Table continues…

	Maximum number supported on VSP 8000 Series
Layer 3 (IPv4)	
IPv4 ARP table	32,000
IPv4 static ARP entries	2,000 for each VRF 10,000 for the switch
IPv4 CLIP interfaces	64
IPv4 route table size	IPv4 and IPv6 route scaling depends on the combination of the ipv6-mode and urpf-mode boot config flags. For more information, see Table 6: IPv4 and IPv6 route scaling on page 83.
IPv4 static routes	1,000 for each VRF 5,000 for the switch
RIP interfaces	200
IPv4 RIP routes	IPv4 and IPv6 route scaling depends on the combination of the ipv6-mode and urpf-mode boot config flags. For more information, see Table 6: IPv4 and IPv6 route scaling on page 83.
IPv4 OSPF routes	IPv4 and IPv6 route scaling depends on the combination of the ipv6-mode and urpf-mode boot config flags. For more information, see Table 6: IPv4 and IPv6 route scaling on page 83.
BGP peers	12
IPv4 BGP routes	IPv4 and IPv6 route scaling depends on the combination of the ipv6-mode and urpf-mode boot config flags. For more information, see Table 6: IPv4 and IPv6 route scaling on page 83.
IPv4 shortcut routes	IPv4 and IPv6 route scaling depends on the combination of the ipv6-mode and urpf-mode boot config flags. For more information, see Table 6: IPv4 and IPv6 route scaling on page 83.
IPv4 route policies	500 for each VRF 5,000 for the switch
IPv4 NLB interfaces	256
IPv4 VRF instances	24
IPv4 UDP forwarding	512
Layer 3 (IPv6)	
IPv6 DHCP Snoop entries in Source Binding Table	1024
IPv6 Neighbor table	8,000
IPv6 static entries in Source Binding Table	256

Table continues…

	Maximum number supported on VSP 8000 Series
IPv6 static neighbor records	256
IPv6 CLIP interfaces	64
IPv6 static routes	1,000
IPv6 OSPFv3 routes - GRT only	IPv4 and IPv6 route scaling depends on the combination of the ipv6-mode and urpf-mode boot config flags. For more information, see Table 6: IPv4 and IPv6 route scaling on page 83.
IPv6 shortcut routes – GRT only	IPv4 and IPv6 route scaling depends on the combination of the ipv6-mode and urpf-mode boot config flags. For more information, see Table 6: IPv4 and IPv6 route scaling on page 83.
IPv6 6in4 configured tunnels	506
RIPng interfaces	48
RIPng routes	IPv4 and IPv6 route scaling depends on the combination of the ipv6-mode and urpf-mode boot config flags. For more information, see Table 6: IPv4 and IPv6 route scaling on page 83.
IPv4/IPv6 Multicast	
Combination of VLANS + number of IPv4 senders + number IPv6 senders (**non-SPBM mode**)	8,192
Combination of L2 VSNs + number of ipv4 senders + number ipv6 senders (**SPBM mode**)	8,192
IGMP/MLD interfaces	4,059
IPv4/IPv6 PIM interfaces	128 (Active)
IPv4/IPv6 PIM Neighbors (GRT Only)	128
IPv4/IPv6 Multicast receivers (per switch)	6,000
IPv4/IPv6 Multicast senders (per switch)	6,000
IPv4/IPv6 Total multicast routes (per switch)	6,000
PIM-SSM static channels	4,000
Static multicast routes	4,000
Multicast enabled Layer 2 VSN	2,000
Multicast enabled Layer 3 VSN	24
Filters and QoS	
Total IPv4 Ingress rules/ACEs (Port/VLAN based, Security/QoS filters)	VSP 8404C = 3,070 Other VSP 8000 Series platforms = 766
Total IPv4 Egress rules/ACEs (Port based, Security filters)	251

Table continues…

	Maximum number supported on VSP 8000 Series
Total IPv6 Ingress rules/ACEs (Port/VLAN based, Security/QoS filters)	VSP 8404C = 2,047 Other VSP 8000 Series platforms = 511
For more information on filter scaling for the VSP 8404C, see Filter scaling for the VSP 8404C on page 83.	
Diagnostics	
Mirrored ports	83 (up to 95 with channelization)
OAM	
FTP sessions (IPv4/IPv6)	4
Rlogin sessions (IPv4/IPv6)	8
SSH sessions (IPv4/IPv6)	8 total (any combination of IPv4 and IPv6 up to 8)
Telnet sessions (IPv4/IPv6)	8
EAPoL 802.1x (clients per port)	32

The following table provides information on IPv4 and IPv6 route scaling. The route scaling does not depend on the protocol itself but rather the general system limitation in different configuration modes.

Table 6: IPv4 and IPv6 route scaling

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

Filter scaling for the VSP 8404C

This section provides more details on filter scaling numbers for the VSP 8404C.

The switch supports a maximum 3070 non-IPv6 ingress ACEs, 2047 IPv6 ingress ACEs, and 251 non-IPv6 egress ACEs.

IPv6 ingress QoS ACL/Filters and IPv6 egress security with QoS ACL/Filters are not supported. If you disable an ACL, the ACL state affects the administrative state of all of the ACEs within it.

ACL scaling

The switch supports the following maximum limits:

- 1024 non-IPv6 ingress ACLs (see Note 1)
- 1024 IPv6 ingress ACLs (see Note 2)

- 126 non-IPv6 egress ACLs (see Note 3)

Note 1: For 1024 non-IPv6 ingress ACLs (inPort or inVlan), the maximum is:

- 1024 ACLs with 1 security ACE each OR
- a combination based on the following rule:

  `num of ACLs <= 1024` AND

  `(num of ACLs + Security ACEs) <= 2048` AND

  `(num of ACLs + QoS ACEs) <= 1024`

This maximum implies a VLAN member count of 1 for inVlan ACLs.

Note 2: For 1024 IPv6 ingress ACLs (inPort), the maximum is:

- 1024 IPv6 ACLs with 1 security ACE each OR
- a combination based on the following rule:

  `num of IPv6 ACLs <= 1024` AND

  `(num of IPv6 ACLs + Security ACEs) <= 2048`

Note 3: For 126 non-IPv6 egress ACLs (outPort), the maximum is:

- 126 ACLs with 1 Security ACE each OR
- a combination based on the following rule:

  `num ACLs <= 126` AND

  `(num ACLs + num security ACEs) <= 252`

This maximum implies a port member counter of 1 for outPort ACLs.

ACE Scaling

The switch supports the following maximum limits:

- 3070 non-IPv6 ingress ACEs (see Note 4)
- 2047 IPv6 ingress ACEs (see Note 5)
- 251 non-IPv6 egress ACEs (see Note 6)

Note 4: For 3070 non-IPv6 ingress ACEs, the theoretical maximum implies the following configuration:

- 1 non-IPv6 ingress ACL with 2047 security ACEs and 1023 QoS ACEs.
- a VLAN member count of 1 for inVlan ACLs
- Non-IPv6 Ingress ACEs supported:

  `[2048(security) - (num of ACLs)] + [1024(QoS) - (num of ACLs)]`

Note 5: For 2047 IPv6 ingress ACEs, the theoretical maximum implies the following configuration:

- 1 IPv6 ingress ACL with 2047 security ACEs
- IPv6 Ingress ACEs supported:

  `[2048(security) - (num of ACLs)]`

Note 6: For 251 non-IPv6 egress ACEs, the theoretical maximum implies the following configuration:

- 1 egress ACL with 251 security ACEs
- a port member count of 1 for outPort ACLs
- Non IPv6 egress ACEs supported:

```
252 - (num egress ACLs)
```

Fabric scaling for VSP 8000 Series

The following table provides fabric scaling information.

Fabric scaling

Attribute	vIST configured	vIST not configured
Number of SPB regions	1	1
Number of BVIDs	2	2
BCB mode (NNI switching supported yes/no)	Yes	Yes
Layer 2 MAC table size (with SPB)	112,000	112,000
SPBM-enabled switches per region (BEB and BCB)	500	500
Number of BEBs this node can share services with (Layer 2 VSNs, Layer 3 VSNs, E-Tree, Multicast, Transparent Port UNI). vIST clusters are counted as 3 nodes. Each Fabric Extend ISIS adjacency reduces this number by 1.	500	500
Number of vIST/IST clusters this node can share I-SIDs with	330	330
Maximum number of Layer 2 VSNs per switch	4,059	4,059
Maximum number of SPB Layer 2/Layer 3 multicast UNI I-SIDs (S,G) per switch	4,000 See Table 7: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured on page 86.	4,000 See Table 7: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured on page 86.
Maximum number of Switched UNI I-SIDs per switch	4,000	4,000

Table continues…

Attribute	vIST configured	vIST not configured
	See Table 7: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured on page 86.	See Table 7: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured on page 86.
Maximum number of FA ISID/ VLAN assignments per port	94	94
Maximum number of Layer 3 VSNs per switch	24	24
Maximum number of Transparent Port UNI per switch	84 (up to 96 with channelization)	84 (up to 96 with channelization)
Maximum number of E-Tree PVLAN UNI per switch	4,059	4,059
Maximum number of NNI interfaces and adjacencies	255	255

Table 7: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured

Number of NNI configured	Number of UNI I-SIDs supported (UNI I-SIDs are used for UNI Layer 2 VSN, Layer 3 VSN,T-UNI, E-Tree, Switched-UNI, S,G for multicast) vIST configured	Number of UNI I-SIDs supported (UNI I-SIDs are used for UNI Layer 2 VSN, Layer 3 VSN,T-UNI, E-Tree, Switched-UNI, S,G for multicast) vIST not configured
Number of NNI = 4	4,000	4,000
Number of NNI = 6	3,500	4,000
Number of NNI = 10	2,900	4,000
Number of NNI = 20	2,000	4,000
Number of NNI = 48	1,000	2,000
Number of NNI = 72	750	1,500
Number of NNI = 100	550	1,100
Number of NNI = 128	450	900
Number of NNI = 250	240	480

File names for VOSS 5.3

This section lists the software files for the VSP 8000 Series platform.

Note:

VOSS 5.3 is supported only on the VSP 8404C hardware platform. It is not supported on other hardware platforms.

Caution:

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

Download images using the binary file transfer.

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

Important:

After you download the software, calculate and verify the md5 checksum. To calculate and verify the md5 checksum on the device, see Calculating and verifying the md5 checksum for a file on a switch on page 88. To calculate and verify the md5 checksum on a Unix or Linux machine, see Calculating and verifying the md5 checksum for a file on a client workstation on page 89. On a Windows machine, use the appropriate Windows utility that is supported on your Windows version.

The encryption modules are included as part of the standard runtime software image file.

The following table lists the files for this release.

Table 8: VSP 8000 Series file names and sizes

Description	File name	Size (in bytes)
Standard runtime software image	VOSS8K.5.3.0.0.tgz	76,636,740
MIB files	• VOSS8K.5.3.0.0_mib.zip • VOSS8K.5.3.0.0_mib.txt	• 1,017,367 • 6,785,495
Supported MIB object names	VOSS8K.5.3.0.0_mib_sup.txt	997,377
EDM Help	VOSSv530_HELP_EDM_gzip.zip	3,293,897
EDM plug-in for COM	VOSSv5.3.0.0.zip	5,310,698
Logs reference	VOSS8K.5.3.0.0_edoc.tar	60,497,920

Open Source software files

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

Table 9: Open Source software files

Product	Master copyright file	Open source base software for 5.3
VSP 8000 Series	VOSS8K.5.3.0.0_oss-notice.html	VOSS8K.5.3.0.0_OpenSource.zip

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

Perform this procedure on a VSP switch to verify that the software files downloaded properly to the switch. Avaya provides the md5 checksum for each release on the Avaya Support website.

Before you begin

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

About this task

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

Procedure

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

   ```
   ls *.tgz
   ```

3. Calculate the md5 checksum for the file:

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

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

Example

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

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

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

Calculate the md5 checksum for the file on the switch:

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

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

Perform this procedure on a Unix or Linux machine to verify that the software files downloaded properly. Avaya provides the md5 checksum for each release on the Avaya Support website.

About this task

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

Procedure

1. Calculate the md5 checksum of the downloaded file:

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

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

2. Verify the md5 checksum of the software suite:

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

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

Example

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

Calculate the md5 checksum of the downloaded file:

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

02c7ee0570a414becf8ebb928b398f51 VSP4K.4.0.40.0.tgz
```

View the md5 checksum of the software suite:

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

a04e7c7cef660bb412598574516c548f VSP4000v4040_HELP_EDM_gzip.zip
ac3d9cef0ac2e334cf94799ff0bdd13b VSP4K.4.0.40.0_edoc.tar
29fa2aa4b985b39843d980bb9d242110 VSP4K.4.0.40.0_mib_sup.txt
c5f84beaf2927d937fcbe9dd4d4c7795 VSP4K.4.0.40.0_mib.txt
ce460168411f21abf7ccd8722866574c VSP4K.4.0.40.0_mib.zip
1ed7d4cda8b6f0aaf2cc6d3588395e88 VSP4K.4.0.40.0_modules.tgz
1464f23c99298b80734f8e7fa32e65aa VSP4K.4.0.40.0_OpenSource.zip
```

```
945f84cb213f84a33920bf31c091c09f VSP4K.4.0.40.0_oss-notice.html
02c7ee0570a414becf8ebb928b398f51 VSP4K.4.0.40.0.tgz
```

Best practices for SPB regarding MSTP

Avaya recommends that NNI ports be used exclusively to transport traffic for SPB-based services and not be configured as members of any VLANs other than SPB BVLANs. Currently, when an IS-IS interface is created on an NNI port or an MLT, MSTP is automatically disabled for MSTI-62 on the port/MLT. But MSTP is not automatically disabled on the NNI ports for the CIST (default MSTI). Avaya recommends that the MSTP be completely disabled on the NNI ports. The following command can be used to disable MSTP completely on the NNI ports.

```
interface gigabitEthernet <port>
no spanning-tree mstp
```

Coexistence of MSTP and SPB based services on NNI ports:

In order to support the coexistence of Non-SPB based services on the NNI ports, the software currently permits adding NNI ports as members of VLANs other than BVLANs. These other VLANs rely on the use of MSTP for Loop prevention. The network operator has to carefully consider the implication of any decision to leave MSTP enabled on the NNI ports. Any MSTP topology changes detected on the NNI ports will impact all services and cause most dynamically learned information on the UNI side to be flushed and relearned. This includes, but is not limited to, all customer MAC and ARP records. This can also cause all the UNI ports on a BEB to be temporarily put into a spanning-tree blocking state before transitioning to a forwarding state again. The net result of this is that MSTP topology changes on the NNI ports adversely impact traffic for SPB based services. For this reason Avaya strongly recommends that the NNI ports be used exclusively for SPB traffic.

Supported browsers

Use the following recommended browser versions to access Enterprise Device Manager (EDM):

- Microsoft Internet Explorer 11
- Mozilla Firefox 43+

Note:

The following earlier browser versions can be used to access EDM (although not recommended):

- Microsoft Internet Explorer 9 and 10
- Mozilla Firefox 37 through 42

User configurable SSL certificates

If you generate a certificate on the switch, you can configure only the expiration time.

If you need to configure other user parameters, you can generate a certificate off the switch and upload the key and certificate files to the `/intflash/ssh` directory. Rename the uploaded files to host.cert and host.key, and then reboot the system. The system loads the user-generated certificates during startup. If the system cannot find host.cert and host.key during startup, it generates a default certificate.

For more information about SSH and SSL certificates, see *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600.

Security modes

The VOSS platforms support three security modes:

- Enhanced secure
- Hsecure
- SSH secure

Enable SSH secure mode to allow only SSH to be used and disable all other protocols which include Telnet, rlogin, FTP, SNMP, TFTP, HTTP, and HTTPS. Enabling this mode disables Telnet, rlogin, FTP, SNMP, TFTP, HTTP, and HTTPS by setting the boot flags for these protocols to off. You can over-ride the configuration and enable required protocols individually for run-time use. The administrator will have to enable required protocols individually for run-time use again following a reboot even if you save the configuration. This is because the SSH secure mode enable takes precedence at the time of reboot and the other protocols will be disabled even though the configuration file has them set to enabled.

Note:

Disabling SSH secure mode will not automatically enable the OA&M protocols that were disabled. The boot flags for the required protocols will have to be individually set to enabled.

The following table lists the differences between enhanced secure mode and hsecure mode.

Table 10: Enhanced secure mode versus hsecure mode

Feature	Enhanced secure	Hsecure
Authentication	Role-based: • admin • privilege • operator	Access-level based: • rwa • rw • ro

Table continues…

Feature	Enhanced secure	Hsecure
	• security • auditor	• l3 • l2 • l1
Password length	Minimum of 8 characters with the exception of the Admin, which requires a minimum of 15 characters	10 characters, minimum
Password rules	1 or 2 upper case, lower case, numeric and special characters	Minimum of 2 upper case, 2 lower case, 2 numeric and 2 special characters
Password expiration	Per-user minimum change interval is enforced, which is programmed by the Administrator	Global expiration, configured by the Admin
Password-unique	Previous passwords and common passwords between users are prevented	The same
Password renewal	Automatic password renewal is enforced	The same
Audit logs	Audit logs are encrypted, and authorized users are able to view, modify, and delete.	Standard operation
SNMPv3	Password rules apply to SNMPv3 Auth&Priv. SNMPv3 is required (V1/V2 disabled)	SNMPv1 and SNMPv2 can be enabled.
EDM	Site Admin to enable or disable	Disabled
Telnet and FTP	Site Admin to enable or disable	The same
DOS attack Prevention	Not available	Prevents DOS attacks by filtering IP addresses and IP address ranges.

Feature licensing

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

If you use a Base License, you do not need to install a license file. If you purchase a Premier License, you must obtain and install a license file. For more information about how to generate a license file, see *Getting Started with Avaya PLDS for Avaya Networking Products*, NN46199-300.

For more information about how to install a license file on the VSP 8000 Series, see *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600.

Important:

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

- Maximum of 63 alphanumeric characters
- No spaces or special characters allowed
- Underscore (_) is allowed
- The file extension ".xml" is required

LACP with Simplified vIST/SPB NNI links

LACP is not recommended on SPB NNI MLT links or on the Simplified Virtual IST.

vIST VLAN IP addresses

Do not configure a Rendezvous Point (RP) or Bootstrap Router (BSR) on the vIST VLAN because you cannot ping them outside of the vIST VLAN subnet. When you enter the **`ip pim enable`** command on the vIST VLAN, the following message displays:

```
WARNING: Please do not use virtual IST VLAN IP address for BSR and RP
related configurations, as unicast packets to virtual IST vlan IP address
from outside of  virtual IST vlan subnet will be dropped. Use Loopback or
CLIP interface IP address for BSR and RP related configurations.
```

show vlan remote-mac-table command output

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

Because all MinM packets that originate from the IST switch use the virtual B-MAC as the source B-MAC, the remote BEB learns the C-MAC against the virtual B-MAC. Because the remote BEB uses the shortest path to the virtual B-MAC, the remote BEB can show the IST peer as a tunnel in the **`show vlan remote-mac-table`** command output.

dos-chkdsk

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

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

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

Auto negotiation settings

VOSS 4.1 and later software requires the same auto negotiation settings on link partners to avoid incorrect declaration of link status. Mismatched settings can cause the links to stay down as well as unpredictable behavior. Ensure the auto negotiation settings between local ports and their remote link partners match before upgrading software to VOSS 4.1 or later.

Interoperability notes for Fabric Attach

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

Table 11: Extending Fabric using Static FA Proxy configuration (ISID/VLAN is manually configured on FA Proxy)

FA Server		FA Proxy	
Product	**Minimum release**	**Product**	**Minimum release**
VSP 4000 Series VSP 7200 Series VSP 8200 VSP 8400	5.0.0.0	ERS 5900	7.0.1
VSP 8404C	5.3.0.0	ERS 5600	6.6.3
		ERS 4800	5.9.2
		ERS 4500	5.7.3

Table 12: Extending Fabric to FA Clients by using FA Proxy

FA Server		FA Proxy		FA Policy	FA Client	
Product	**Minimum release**	**Product**	**Minimum release**		**Product**	**Minimum release**
VSP 4000 Series VSP 7200 Series VSP 8200 VSP 8400	5.0.0.0	ERS 5900	7.0.1	IDE Release 9.1 (See Note below)	AP9100	7.2.5
VSP 8404C	5.3.0.0	ERS 5600	6.6.3			
		ERS 4800	5.9.2			
		ERS 4500	5.7.3			

Note:

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

Interoperability considerations for IS-IS external metric

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

Important:

Note the following before turning on IS-IS external metric if the SPB network has switches running a release other than VOSS 5.0.

- There are no special release or product type implications if the switch does not have IP shortcuts or L3VSN enabled. For example, this applies to L2 only BEBs and BCBs.
- There are no special release or product type implications if the L3VSN in which routes are being advertised with a metric-type of external is not configured on the switch.
- If a switch running a VOSS release that is prior to VOSS 5.0 but VOSS 4.2.1 or later, it will treat all IS-IS routes as having metric-type `internal`, irrespective of the metric-type (internal or external) used by the advertising BEB in its route advertisement.
- Switches running VSP 9000 release 4.1.0.0 or later will treat all IS-IS routes as having metric-type `internal`, irrespective of the metric-type (internal or external) used by the advertising BEB in its route advertisement.

- Switches running VOSS releases prior to 4.2.1.0 may not correctly install IS-IS routes in a L3VSN if any routes are advertised with metric-type external are advertised in that L3VSN by other BEBs in the network. L3VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to GRT.
- Switches running VSP 9000 releases prior to 4.1.0.0 may not correctly install IS-IS routes in a L3VSN if any routes are advertised with metric-type external are advertised in that L3VSN by other BEBs in the network. L3VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to GRT.
- Switches running any ERS 8800 release may not correctly install IS-IS routes in of a L3VSN if any routes are advertised with metric-type external are advertised in that L3VSN by other BEBs in the network. L3VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to GRT.

Chapter 5: Known issues and limitations

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

Known issues in this release

This section identifies the known issues in this release for the VSP 8000 Series product.

Device related issues

Table 13: Known issues

Issue number	Description	Workaround
wi01144867	On the port that is removed from a T-UNI LACP MLT, non T-UNI configuration is blocked as a result of T-UNI consistency checks.	When a port is removed from a T-UNI LACP MLT, the LACP key of the port must be set to `default`.
wi01173026	A reboot with verbose configuration does not allow you to delete a VRF.	This issue occurs only if you save the configuration file in verbose mode and reboot the switch in that configuration. This situation is unlikely to exist; verbose mode is used more as a diagnostic tool. This issue does not impact functionality.
wi01173136	T1 SFP: Shutting down the T1 link from one end of the VSP 4000 or VSP 7200 Series or VSP 8000 Series does not shut down the link at the remote end. You may experience traffic loss if the remote side of the link is not shut down.	This issue occurs only when a T1 SFP link from one end is shutdown. Enable a dynamic link layer protocol such as LACP or VLACP on both ends to shut the remote end down too. As an alternative, administratively disable both ends of the T1 SFP link to avoid the impact.
wi01175118	On a MACsec enabled port, you may see delayed packets when the MACsec port is kept running for more than 12 hours. This delayed packet counter may also increment when there is complete reordering	None.

Table continues…

Issue number	Description	Workaround
	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.	
wi01195988	You cannot use EDM to issue ping or traceroute commands for IPv6 addresses.	Use ACLI to initiate ping and traceroute.
wi01196000	You cannot use EDM to issue ping or traceroute commands for IPv4 addresses.	Use ACLI to initiate ping and traceroute.
wi01197712	On the 40-gigabit ports, the small metallic fingers that surround the ports are fragile and can bend out of shape during removal and insertion of the transceivers. When the fingers are bent, they prevent the insertion of the QSFP+ transceiver. **Note:** This issue is specific to VSP8404QQ ESMs.	Insert the QSFP+ carefully. If the port gets damaged, it needs to be repaired.
wi01208650	The Console gets disconnected frequently when you enable screen trace (trace screen enable). The error displayed is `Forced log-out after 65535 secs`.	None
wi01209346	In an IGMP snoop environment, after dynamically downgrading the IGMP version to version 2 (v2), when you revert back to version 3 (v3), the following is observed: • The multicast traffic does not flow. • The sender entries are not learned on the local sender switch. • The Indiscard packet count gets incremented on the **`show int gig error`** statistics command.	Use a v3 interface as querier in a LAN segment which has snoop– enabled v2 and v3 interfaces.
wi01209604	From EDM, you cannot perform a Layer 2 IP PING for an IPv6 address. EDM displays the following error: `No next Hop address found for ip address provided`.	Use the ACLI perform a Layer 2 IP PING.
wi01210104	In EDM, you cannot select multiple 40–gigabit ports or a range of ports that includes 40–gigabit ports to graph or edit. You need to select them and edit them individually.	None.

Table continues…

Issue number	Description	Workaround
	Note: This issue applies to products that support 40 Gbps ports.	
wi01212099	In the COM EDM Plugin command, the Layer 2 Traceroute IPv6 does not work properly and gives the error, `No Such Name`.	Use the ACLI to initiate the Layer 2 Traceroute for IPv6.
wi01212115	On EDM, the port LED for channelized ports only shows the status of sub-port #1, but not the rest of the sub-ports. When you remove sub-port #1, and at least one other sub-port is active and online, the LED color changes to amber, when it should be green because at least one other sub-ports is active and online. The LED only shows the status of sub-port #1.	None.
wi01212860	An intermittent link-flap issue can occur in the following circumstance for the copper ports of the VSP 7254XTQ or the 8424XT ESM for VSP 8400: If you use a crossover cable and disable auto-negotiation, the port operates at 100 Mbps. A link flap issue can occur intermittently and link flap detect will shutdown the port.	Administratively shutdown, and then reenable the port. **Note:** Avaya recommends that you use auto-negotiation. Disabling auto-negotiation on these ports is not a recommended configuration.
wi01214025	Traffic is forwarded to IGMP v2 SSM group, even after you delete the IGMP SSM-map entry for the group.	If you perform the delete action first, you can recreate the SSM-map record, and then disable the SSM-map record. The disabled SSM-map record causes the receiver to timeout because any subsequent membership reports that arrive and match the disabled SSM-map record are dropped. You can delete the SSM-map record after the receivers time out.
wi01214772	The 4 byte AS confederation identifier and peers configuration are not retained across a reboot. This problem occurs when 4 Byte AS is enabled with confederation.	Reconfigure the 4 byte AS confederation identifier and peers on the device, and reboot.
wi01215220	After you enable enhanced secure mode, and log in for the first time, the system prompts you to enter a new password. If you do not meet the minimum password requirements, the following system output message appears: `Password should contain a minimum of 2 upper and lowercase letters, 2 numbers and 2 special characters`	None.

Table continues…

Issue number	Description	Workaround
	`like !@#$%^*(). Password change aborted. Enter the New password:` The system output message does not display the actual minimum password requirements you need to meet, which are configured on your system. The output message is an example of what the requirements may need to meet. The actual minimum password requirements you need to meet are configured on your system by the administrator.	
wi01215773	The switch provides an NTP log message that indicates that the NTP server did not synchronize, even though one of the NTP servers synchronized correctly and the NTP stats show that it did.	None.
wi01216535	The `router ospf` entry always appears in the configuration file regardless of whether OSPF is configured. This line does not perform any configuration and has no impact on the running software.	None.
wi01216550	When you use Telnet or SSH to connect to the switch, it can take up to 60 seconds for the login prompt to appear. However, this situation is very unlikely to happen, and it does not appear in a standard normal operational network.	Do not provision DNS servers on a switch to avoid this issue altogether.
wi01217251	If you configure egress mirroring on NNI ports, you do not see the MAC-in-MAC header on captured packets.	Use an Rx mirror on the other end of the link to see the packets.
wi01217347	A large number of IPv6 VRRP VR instances on the same VLAN can cause high CPU utilization.	Do not create more than 10 IPv6 VRRP VRs on a single VLAN.
wi01217871	If you attach the QSFP+ end of a passive breakout cable to a VSP 4000 or VSP 7200 Series or VSP 8000 Series switch, and the SFP+ ends of the cable to a VSP 9000 running Release 4.0.1, the output for the **`show pluggable-optical-modules basic`** command on the VSP 9000 shows an incorrect vendor name and part number. The incorrect information also appears in EDM under the **Edit** > **Port** > **General** menu path.	This issue will be fixed in a future VSP 9000 software release.
wi01221817	If you disable IPv6 on one RSMLT peer, the switch can intermittently display `COP-SW ERROR` and `RCIP6 ERROR` error messages.	None.

Table continues…

Issue number	Description	Workaround
	This issue has no impact.	
wi01222078	If you delete the SPBM configuration and re-configure SPBM using the same nickname but a different ISIS system id without rebooting, the switch displays an error message.	Reboot the switch after you delete the SPBM configuration.
wi01223719	You cannot use EDM to configure SSH rekey and enable or disable SFTP.	Use ACLI to configure SSH rekey and enable or disable SFTP.
wi01223723	EDM displays the user name as Admin, even though you login using a different user name.	None.
wi01223759	You cannot use EDM to view the IPv6 DHCP relay counters.	Use ACLI to view the IPv6 DHCP relay counters.
wi01224076	When you re-enable insecure protocols in the ACLI SSH secure mode, the switch does not display a warning message.	None.
wi01224644	EDM displays the IGMP group entry that is learnt on vIST MLT port is as TX-NNI.	Use ACLI to view the IGMP group entry learnt on vIST MLT port.
wi01225023	When port-lock is enabled on the port and re-authentication on the EAP client fails, the port is removed from the radius assigned VLAN. This adds the port to default VLAN and displays an error message. This issue has no impact.	The error message is incorrect and can be ignored.
wi01225232	When an operational SMLT is removed from a TUNI ISID and is not added to any other VLAN or TUNI ISID, then spanning tree is enabled on this SMLT interface. Spanning tree is disabled when added to VLAN or TUNI ISID. This issue has no impact.	Disable SMLT ports and then remove them from TUNI ISID.
wi01225310	When ISIS is disabled on one of the VIST peer nodes with RSMLT interfaces and it has ECMP routes with the RSMLT Peer as the next hop, the ECMP routes that are being replaced during the transition of the ISIS state now will have a next hop of the local interface. This results in an error message `COP-SW ERROR ercdProcIpRecMsg: Failed to Replace IP Records`.	Enable ISIS on both the vIST peers.
wi01226335	In a rare scenario in Simplified vIST configuration when vIST state is toggled immediately followed by vIST MLT ports are toggled, one of the MLT ports will go into blocking state resulting in failure to process data packets hashing to that link.	Before enabling vIST state ensure all VIST MLT ports are shut and re-enabled after vIST is enabled on the DUT.

Table continues…

Issue number	Description	Workaround
wi01226433 wi01226437	When you configure a scaled Layer 3 VSN (24 Layer 3 VSN instances), route leaking from GRT to VRF on the local DUT does not happen. The switch displays an incorrect error message `Only 24 L3 VSNs can be configured`.	None.
wi01230533 wi01230953 wi01232817	When you use Fabric Extend over IP (FE-IP) and Fabric Extend over L2 VLAN (FE-VID) solution, if you change the ingress and egress .1p map, packets may not follow correct internal QoS queues for FE tunnel to FE tunnel, or FE tunnel to regular NNI traffic. .	Do not change the default ingress and egress .1p maps when using Fabric Extend. With default ingress and egress . 1p maps, packets follow the correct internal QoS when using the Fabric Extend feature
wi01232095	EDM and ACLI show different local preference values for a BGP IPv6 route. EDM displays path attributes as received and stored in the BGP subsystem. If the attribute is from an eBGP peer, the local preference appears as zero. ACLI displays path attributes associated with the route entry, which can be modified by a policy. If a route policy is not configured, the local preference shows the default value of 100.	None
wi01232581	You cannot use EDM to enable or disable ASG. You can only view ASG status.	Use ACLI to enable or disable ASG.
wi01233201	If the I-SID associated with a Switched UNI or Fabric Attach port does not have a platform VLAN association and you disable Layer 2 Trusted, then the non IP traffic coming from that port does not take the port QoS and still uses the .1p priority in the packet.	None
wi01233828 VOSS-1487	If you establish an SSH connection to a switch, and then use that switch to create a Telnet session with another device, when you exit the Telnet session, the original SSH connection can stop responding.	Halt the original SSH connection and reconnect.
wi01234422	If you improperly close an SSH session, the session structure information does not clear and the client can stop functioning.	Disable and enable SSH.
wi01234623	VSP 7200 Series and VSP 8000 Series do not Support Fabric Extend over Layer 2 VLAN (FE-VID) logical interface configuration over an MLT interface.	None

Table continues…

Issue number	Description	Workaround
wi01234739	If you apply an ipv6-out-route-map on a BGP peer to filter a particular IPv6 prefix range with a match network condition, it does not filter the full prefix range.	Configure the incoming policy to filter incoming advertised routes on BGP+ peers.
wi01234872	The **`show debug-file all`** command is missing on VSP 7200 Series and VSP 8000 Series platforms.	None
wi01234873	The system does not generate a log message, either in the log file or on screen, when you run the **`flight-recorder`** command.	None
wi01235018	If you use an ERS 4850 FA Proxy with a VOSS FA Server, a mismatch can exist in the show output for tagged management traffic. The ERS device always sends traffic as tagged. The VOSS FA Server can send both tagged and untagged. For untagged, the VOSS FA Server sends VLAN ID 4095 in the management VLAN field of the FA element TLV. The ERS device does not recognize this VLAN ID and so still reports the traffic as tagged.	There is no functional impact.
wi01235053	If you use EDM to create an ACL filter, the ACL tab does not automatically refresh to show the new filter.	Click **Refresh** on the ACL tab to force a data refresh.

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

VOSS-2253	Trace level command does not list module IDs when '?' is used.	To get the list of all module IDs, type “trace level” and then press Enter.

Table continues…

Issue number	Description	Workaround
VOSS-2014	IPV6 MLD Group is learned for Link-Local Scope Multicast Addresses. This displays additional entries in the Multicast routing tables.	None

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

VOSS-2285	When on BEB, continuously pinging IPv6 neighbor address using ACLI command ping -s, ping packets don’t drop, but see "no answer" messages.	Restart the ping. Avoid intensive CPU processing.
VOSS-1706	EAPOL: Untagged traffic not honouring port QOS for Layer 2 trusted/ Layer 3 untrusted. Issue is only seen on EAPOL enabled port.	None
VOSS-2128	EAP Security and Authentication tabs displays additional information with internal values populated which is not useful for the end user.	There is no functional impact. Ignore the additional information in EDM. Use ACLI command. "show eapol port interaface” to get port status.
VOSS-2333	L2 ping to Virtual BMAC (VBMAC) fails, if the VBMAC is reachable via L2core.	None
VOSS-2279	When IPv6 neighbor device boots up, the following error message occurs in the peer device console:	There is no functional impact. Port shut/no shut which recovers the traffic

Table continues…

Issue number	Description	Workaround
	`GlobalRouter COP-SW ERROR ercdProcIpv6RouteMsg: Failed to Delete IPV6 Record - Ip: fe80:0:0:8dc:b2ad:aaff:fe55:1b91, NextHop:0:0:0:0:0:0:0:0, mask: 128`	works even when the switch is in error state.
VOSS-2415	There is no option in the "Insert V3 Interface" screen of EDM to insert a VRRP v3 interface for IPv6. The two check boxes in the screen are disabled.	There is no functional impact. EDM has two menus of IP and IPv6 and this functionality is available there along with other features.
VOSS-2422	When BGP Neighbor times out, the following error message occurs: `CP1 [03/11/16 13:43:39.084:EST] 0x000b45f2 00000000 GlobalRouter SW ERROR ip_rtdeleteVrf: orec is NULL!`	There is no functional impact. Ignore the error message.
VOSS-2208	While performing CFM L2 traceroute between two BEB's via a transit BCB, transit BCB's hop is not seen, if the transit BCB has **ISIS adjacencies over FE l3core with both** source BEB and destination BEB.	None
VOSS-2270 wi01227920 wi01230534	The packet internal CoS is derived incorrectly for packets sourced from a brouter port when the CoS should be derived from the port level QoS. The following list identifies scenarios that derive the internal CoS from the port QoS: • Untagged non-IP packet • Untagged IP packet, and the source port is Layer 3 untrusted • Tagged non-IP packet and the source port is Layer 2 untrusted • Tagged IP packet and the source port is Layer 3 untrusted and Layer 2 untrusted.	Use the port default QoS configuration for the brouter port. The port default configuration is Layer 2 trusted and Layer 3 trusted, and under this configuration, only the first scenario in the list is still an issue. The other scenarios do not occur.
VOSS-2444	The output of the **`show ip mroute stats [group address]`** wraps to an additional line. Four columns of data are on one line and the fifth column *AverageSize* wraps to an additional line. There is also an extra line feed in the column header.	None

Table continues…

Issue number	Description	Workaround
VOSS-4114 VOSS-4116 VOSS-4972 VOSS-5258	You cannot use FireFox 50 or newer to connect to EDM using HTTPS.	Do not use these newer browser versions until Release 6.1.
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-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-5467	If a MinM Unicast packet (destined to a virtual BMAC) is sent over an FE tunnel to a vIST paired BEB, and that destination BEB has not yet learned the customer destination MAC, then the flooded packet is not received by its vIST peer.	Ensure that you flush the customer MAC addresses in the particular VLAN or I-SID on both the vIST peer BEBs on which the FE tunnel is terminated.
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 that 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-5670	In an SPBM environment, when you execute the traceroute command to a destination IP address learned using inter-VRF routing, the traceroute fails.	None
VOSS-5855	You cannot use SFTP to download the alarm log files or the output of the `show fulltech file <filename>` command.	Use FTP or TFTP instead, to download the files.
VOSS-5856	On the switch, when you insert a 100 Gbps DAC into a 40 Gbps Ethernet port, the log message correctly indicates that the supported operational speed is 40 Gbps.	None

Table continues…

Issue number	Description	Workaround
	However, the output of the **show interfaces gigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}** command for the same port shows the admin speed as 100000 instead of 40000. The operational speed is correctly displayed as 40000 only after the port state is up. This inconsistency is only in the command output display. There is no functional impact.	

Limitations in this release

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

Limitations for VSP 8404C

The following table provides a description of the limitation or behavior and the work around, if one exists.

Table 14: Limitations for VSP 8404C

Behavior	Description	Workaround
For system power up	The VSP 8404C does not power up successfully if the 8402CQ ESM is not inserted in the system.	Ensure that the 8402CQ ESM is inserted in the system *before* you power up the VSP 8404C.

General limitations and expected behaviors

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

Table 15: General limitations and expected behaviors

WI number	Description
wi01068569	The system displays a warning message that routes will not inject until the apply command is issued after the enable command. The warning applies only after you enable redistribution, and not after you disable redistribution. For example, `4k2:1(config)#isis apply redistribute direct vrf 2`.
wi01112491	IS-IS enabled ports cannot be added to an MLT. The current release does not support this configuration.
wi01122478	Stale SNMP server community entries for different VRFs appear after reboot with no VRFs . On a node with a valid configuration file saved with more than the default vrf0 , SNMP community entries for that VRF are created and maintained in a separate text

Table continues…

WI number	Description
	file, snmp_comm.txt, on every boot. The node reads this file and updates the SNMP communities available on the node. As a result, if you boot a configuration that has no VRFs, you may still see SNMP community entries for VRFs other than the globalRouter vrf0 .
wi01137195	A static multicast group cannot be configured on a Layer 2 VLAN before enabling IGMP snooping on the VLAN. After IGMP snooping is enabled on the Layer 2 VLAN for the first time, static multicast group configuration is allowed, even when IGMP snooping is disabled later on that Layer 2 VLAN.
wi01138851	Configuring and retrieving licenses using EDM is not supported.
wi01142142	When a multicast sender moves from one port to another within the same BEB or from one VIST peer BEB to another, with the old port operationally up, the source port information in the output of the **`show ip igmp sender`** command is not updated with new sender port information. You can perform one of the following workarounds: • On an IGMP snoop-enabled interface, you can flush IGMP sender records. ⚠ **Caution:** Flushing sender records can cause a transient traffic loss. • On an IGMP-enabled Layer 3 interface, you can toggle the IGMP state. ⚠ **Caution:** Expect traffic loss until IGMP records are built after toggling the IGMP state.
wi01145099	IP multicast packets with a time-to-live (TTL) equal to 1 are not switched across the SPB cloud over a Layer 2 VSN. They are dropped by the ingress BEB. To prevent IP multicast packets from being dropped, configure multicast senders to send traffic with TTL greather than 1.
wi01171670	Telnet packets get encrypted on MACsec enabled ports.
wi01210217	The command **`show eapol auth-stats`** displays LAST-SRC-MAC for NEAP sessions incorrectly.
wi01211415	In addition to the fan modules, each power supply also has a fan. The power supply stops working if a power supply fan fails, but there is no LED or software warning that indicates this failure. Try to recover the power supply fan by resetting the switch. If the fan does not recover, then replace the faulty power supply.
wi01212034	When you disable EAPoL globally: • Traffic is allowed for static MAC configured on EAPoL enabled port without authentication. • Static MAC config added for authenticated NEAP client is lost.
wi01212247	BGP tends to have many routes. Frequent additions or deletions impacts network connectivity. To prevent frequent additions or deletions, reflected routes are not

Table continues…

WI number	Description
	withdrawn from client 2 even though they are withdrawn from client 1. Disabling Route-reflection can create blackhole in the network. Workaround: Bounce the BGP protocol globally.
wi01212585	LED blinking in EDM is representative of, but not identical to, the actual LED blinking rates on the switch.
wi01213040	When you disable auto-negotiation on both sides, the 10 Gbps copper link does not come up.
wi01213066 wi01213374	EAP and NEAP are not supported on brouter ports.
wi01213336	When you configure `tx` mode port mirroring on T-UNI and SPBM NNI ports, unknown unicast, broadcast and multicast traffic packets that ingress these ports appear on the mirror destination port, although they do not egress the mirror source port. This is because `tx` mode port mirroring happens on the mirror source port *before* the source port squelching logic drops the packets at the egress port.
wi01219295	SPBM QOS: Egress UNI port does not follow port QOS with ingress NNI port & Mac-in-Mac incoming packets.
wi01219658	The command **`Show khi port-statistics`** does not display the count for NNI ingress control packets going to the CP.
wi01223526	ISIS logs duplicate system ID only when the device is a direct neighbor.
wi01223557	Multicast outage occurs on LACP MLT when simplified vIST peer is rebooted. You can perform one of the following work arounds: • Enable PIM on the edge. • Ensure that IST peers are either RP or DR but not both.
wi01224683 wi01224689	Additional link bounce may occur on the following ports, when toggling links or during cable re-insertion: • VSP 7254XSQ 10 Gbps port • VSP 7254XSQ and VSP7254XTQ 40Gig optical cables and 40 Gbps break out cables • VSP 8200 and VSP 8400 40 Gbps ports with optical cable • VSP 8200 and VSP 8400 40 Gbps ports with optical breakout cable
wi01229417	Origination and termination of IPv6 6-in-4 tunnel is not supported on a node with vIST enabled.
wi01232578	When SSH keyboard-interactive-auth mode is enabled, the server generates the password prompt to be displayed and sends it to the SSH client. The server always sends an expanded format of the IPv6 address. When SSH keyboard-interactive-auth mode is disabled and password-auth is enabled, the client itself generates the password prompt, and it displays the IPv6 address format used in the **`ssh`** command.

SSH connections

VOSS 4.1.0.0 and VOSS 4.2.0.0 SSH server and SSH client support password authentication mode.

VOSS 4.2.1.0 changed the SSH server from password authentication to keyboard-interactive. VOSS 4.2.1.0 changed the SSH client to automatically support either password authentication or keyboard-interactive mode.

In VOSS 4.2.1.0, you cannot configure the SSH server to support password authentication. This limitation creates a backward compatibility issue for SSH clients that do not support keyboard-interactive mode, including SSH clients that are part of pre-VOSS 4.2.1.0 software releases. For example, VOSS 4.1.0.0 SSH clients, VOSS 4.2.0.0 SSH clients, and external SSH clients that only support password authentication cannot connect to VOSS 4.2.1.0 SSH servers.

This issue is addressed in software release VOSS 4.2.1.1 and later. The default mode of the SSH server starting from VOSS 4.2.1.1 is changed back to password authentication. Beginning with VOSS 5.0, you can use an ACLI command to change the SSH server mode to keyboard-interactive. For more information about how to configure the SSH server authentication mode, see *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 or *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600.

Note:

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

See the following table to understand SSH connections between specific client and server software releases.

Client software release	Server software release	Support
VOSS 4.1.0.0	VOSS 4.2.0.0	Supported
VOSS 4.1.0.0	VOSS 4.2.1.0	Not supported
VOSS 4.2.0.0	VOSS 4.2.1.0	Not supported
VOSS 4.1.0.0	VOSS 4.2.1.1	Supported
VOSS 4.2.0.0	VOSS 4.2.1.1	Supported

Chapter 6: Resolved issues

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

Fixes from previous releases

VOSS 5.3 incorporates all fixes from prior releases, up to and including VOSS 5.1.1.

Table 16: Resolved issues in this release

Issue number	Description
wi01235322 VOSS-1682	Secure Copy (SCP) file transfers on VSP switches, running VOSS 5.0, stall intermittently due to 100% thread utilization of the SCP process, which is responsible for file transfer. This problem is seen intermittently when the transfer is initiated from SSH client versions earlier than OpenSSH_5.0, or for files with size of 1 GB or larger. For client versions later than OpenSSH_5.0, this stall condition is rare for file sizes up to 500 MB and has not been seen for files with sizes that are typically transferred to and from VOSS switches. The use of some older client versions such as the ones shown in the following list always result in stalled file transfers: • Sun_SSH_1.1, SSH protocols 1.5/2.0, OpenSSL 0x0090704f • OpenSSH_3.9p1, OpenSSL 0.9.7a Feb 19 2003 The recommended client and file size range to avoid this problem is to use Open SSH client version later than 5.0 and file sizes up to 500 MB. This issue was resolved in this release.
VOSS-1747	On a VSP 8404 with MLT on 10G ports on an 8424XT or 8424XTQ module, multiple VLANs that have the MLT as a member of the VLAN, there is a possibility that a copy of the IP multicast traffic may not be sent on all VLANs that have a receiver on the MLT. This issue was resolved in this release.
VOSS-1758	After changing ISIS System-ID, it is possible that CFM L2 ping will not work properly. This issue was resolved in this release.
VOSS-2185	MAC move of the client to the new port does not automatically happen when you move a Non-EAP client authenticated on a specific port to another EAPoL or Non-EAP enabled port. This issue was resolved in this release.

Table continues…

Issue number	Description
VOSS-2237	Configuring NTP server with wrong key value, error message occurs in two scenarios. • When passwords (keys) start with a special 9 character instead of alphanumeric characters. • When passwords (keys) contain a space between characters. Error message: `setting NtpKeyTbl, Operation not allowed` This issue was resolved in this release.

Chapter 7: Resources

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Documentation

See *Documentation Reference for VSP Operating System Software*, NN47227-100 for a list of documentation for all VOSS products.

For installation and initial setup information of the Open Networking Adapter (ONA), refer to the Quick Install Guide that came with your ONA.

Note:

The ONA works only with the Avaya Virtual Services Platform 4000 Series.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com/.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

  ✻ **Note:**

  Videos are not available for all products.

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx.
3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
   - Whole Words Only

- Case-Sensitive
- Include Bookmarks
- Include Comments

6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Subscribing to e-notifications

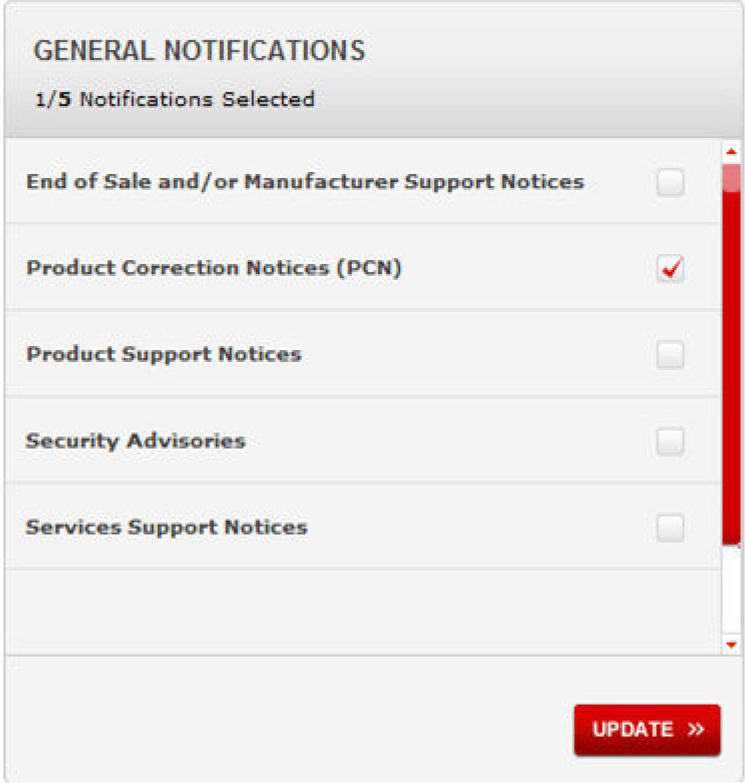
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Ethernet Routing Switch 5000 Series.

Procedure

1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.

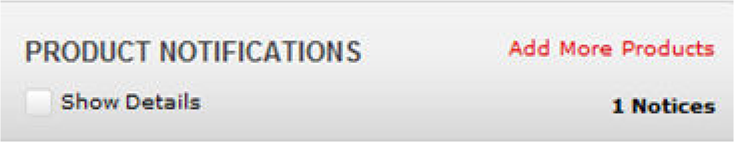


GENERAL NOTIFICATIONS

1/5 Notifications Selected

- End of Sale and/or Manufacturer Support Notices □
- Product Correction Notices (PCN) ☑
- Product Support Notices □
- Security Advisories □
- Services Support Notices □

6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.

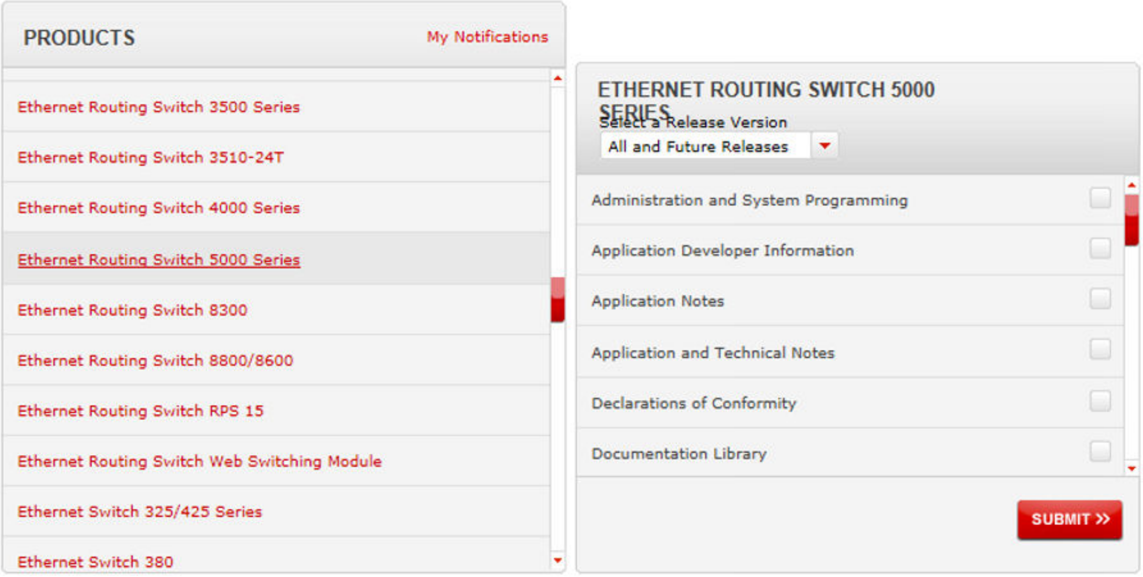


PRODUCT NOTIFICATIONS

□ Show Details

1 Notices

8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.


PRODUCTS
My Notifications
Ethernet Routing Switch 3500 Series
Ethernet Routing Switch 3510-24T
Ethernet Routing Switch 4000 Series
Ethernet Routing Switch 5000 Series
Ethernet Routing Switch 8300
Ethernet Routing Switch 8800/8600
Ethernet Routing Switch RPS 15
Ethernet Routing Switch Web Switching Module
Ethernet Switch 325/425 Series
Ethernet Switch 380
ETHERNET ROUTING SWITCH 5000 SERIES
Administration and System Programming □
Application Developer Information □
Application Notes □
Application and Technical Notes □
Declarations of Conformity □
Documentation Library □
SUBMIT »

Select a Release Version: All and Future Releases

11. Click **Submit**.

Appendix A: Related information for 5.3

Related information

The following section contains information related to the current release.

Overview of features by release and platform

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

Note:

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

Feature introduction

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

Features	Release by platform series	
	VSP 8200	VSP 8400
Operations and management		
Avaya CLI (ACLI) For more information, see *Using ACLI and EDM on VSP Operating System Software*, NN47227-103.	4.0	4.2
Channelization of 40 Gbps ports For more information, see *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600.	4.2	4.2
Channelization of 100 Gbps ports	N/A	N/A
Configuration and Orchestration Manager (COM) For more information, see Avaya Configuration and Orchestration Manager (COM) documentation, http://support.avaya.com/.	4.0	4.2
Domain Name Service (DNS) client (IPv4)	4.0	4.2

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600		
DNS client (IPv6) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.1	4.2
The encryption modules file is included in the runtime software image file; it is not a separate file.	4.2	4.2
Enable or disable ICMP Broadcast/Multicast For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505 • *Configuring IPv6 Routing on VSP Operating System Software*, NN47227-507	5.1	5.1
Enable/disable IP Source Routing For more information, see the following documents: • *Configuring IP Routingon Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505 • *Configuring IPv6 Routing on VSP Operating System Software*, NN47227-507	5.1	5.1
Enhanced Secure mode For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.2	4.2
Enterprise Device Manager (EDM) For more information, see *Using ACLI and EDM on VSP Operating System Software*, NN47227-103.	4.0	4.2

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
EDM representation of physical LED status For more information, see the following documents: • *Installing Avaya Virtual Services Platform 4850GTS Series*, NN46251-300 • *Installing Avaya Virtual Services Platform 4450GTX-HT-PWR+ Switch*, NN46251–304 • *Installing Avaya Virtual Services Platform 4450GSX-PWR+ Switch*, NN46251-307 • *Installing the Avaya Virtual Services Platform 7200 Series*, NN47228-302 • *Installing the Avaya Virtual Services Platform 8000 Series*, NN47227-300	4.2	4.2
File Transfer Protocol (FTP) server/client (IPv4) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.0	4.2
FTP server/client (IPv6) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.1	4.2
Flight Recorder (for system health monitoring) For more information, see the following documents: • *Troubleshooting of Avaya Virtual Services Platform 4000 Series*, NN46251-700 • *Troubleshooting Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-700	4.0	4.2
IEEE 802.1ag Connectivity Fault Management (CFM) • Layer 2 Ping • TraceRoute • TraceTree For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.0	4.2

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
Extensible Authentication Protocol (EAP) and EAP over LAN (EAPoL) For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.1	4.2
Extensible Authentication Protocol over LAN (EAPol) MHMA-MV For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	5.1	5.1
Key Health Indicator (KHI) For more information, see the following documents: • *Fault Management of Avaya Virtual Services Platform 4000 Series*, NN46251-702 • *Managing Faults on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-702	4.0	4.2
Logging (log to file and syslog [IPv4]) For more information, see the following documents: • *Fault Management of Avaya Virtual Services Platform 4000 Series*, NN46251-702 • *Managing Faults on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-702	4.0	4.2
Logging (log to file and syslog [IPv6]) For more information, see the following documents: • *Fault Management of Avaya Virtual Services Platform 4000 Series*, NN46251-702 • *Managing Faults on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-702	4.1	4.2
Mirroring (port and flow-based) For more information, see the following documents: • *Troubleshooting of Avaya Virtual Services Platform 4000 Series*, NN46251-700 • *Troubleshooting Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-700	4.0	4.2
Network Time Protocol (NTP)	4.0	4.2

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600		
Non EAPoL MAC RADIUS authentication For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.2.1	4.2.1
NTP with SHA Authentication For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series* • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600 .	5.1	5.1
PoE/PoE+ Allocation Using LLDP For more information, see the following document: • *Administration for Avaya Virtual Services Platform 4000 Series* .	N/A	N/A
RADIUS, community-based users (IPv4) For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.0	4.2
RADIUS (IPv6) For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.1	4.2
Remote Login (Rlogin) server/client (IPv4) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600	4.0	4.2

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
• *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600		
Rlogin server (IPv6) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.1	4.2
Remote Monitoring 1 (RMON1) for Layer 1 and Layer 2 ✱ **Note:** Release 5.0 and 5.1 do not support RMON1.	4.0	4.2
Remote Monitoring 2 (RMON2) for network and application layer protocols For more information, see the following documents: • *Performance Management of Avaya Virtual Services Platform 4000 Series*, NN46251-701 • *Monitoring Performance on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-701	4.2	4.2
Remote Shell (RSH) server/client For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.0	4.2
Russia summer time zone change For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.2	4.2
Secure Copy (SCP) ✱ **Note:** Release 4.2 and 4.2.1 do not support SCP. For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600	4.0	5.0

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
• *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600		
Secure FTP (SFTP) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.0	4.2
Secure hash algorithm 1 (SHA-1) and SHA-2 For more information, see the following documents: • *Configuring OSPF and RIP on Avaya Virtual Services Platform 4000 Series*, NN46251-506 • *Configuring OSPF and RIP on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-506	4.2	4.2
Secure Shell (SSH) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.0	4.2
Secure Sockets Layer (SSL) certificate management For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.1	4.2
SMTP for email notification For more information, see Features in release 5.3 on page 13.	N/A	5.3
SSH (IPv6) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.1	4.2
SSH rekey	5.1	5.1

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600		
SLA Mon™ For more information, see the following documents: • *Performance Management of Avaya Virtual Services Platform 4000 Series*, NN46251-701 • *Monitoring Performance on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-701	4.1	4.2
Simple Loop Prevention Protocol (SLPP) For more information, see the following documents: • *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 4000 Series*, NN46251-500 • *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-500	4.0	4.2
Simple Network Management Protocol (SNMP) v1/2/3 (IPv4) For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.0	4.2
SNMP (IPv6) For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.1	4.2
SoNMP (Avaya topology discovery protocol) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.0	4.2
`spbm-config-mode` boot flag	4.0.1	4.2

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
For more information, see the following documents: • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series* , NN46251-504 • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-504		
TACACS+ For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.1	4.2
Telnet server/client (IPv4) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.0	4.2
Telnet server/client (IPv6) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.1	4.2
Trivial File Transfer Protocol (TFTP) server/client (IPv4) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.0	4.2
TFTP server/client (IPv6) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.1	4.2
Virtual Link Aggregation Control Protocol (VLACP)	4.0	4.2

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on VSP Operating System Software*, NN47227-503.		
QoS per queue rate limiting For more information, see the following documents: • *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series*, NN46251-502 • *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-502	5.1.1	5.1.1
Layer 2		
Avaya switch cluster (multi-chassis LAG) • Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on VSP Operating System Software*, NN47227-503.	4.0	4.2
Bridge Protocol Data Unit (BPDU) Guard For more information, see Features in release 5.3 on page 13.	N/A	5.3
Entity MIB — Physical Table For more information, see Features in release 5.3 on page 13.	N/A	5.3
First Hop Security For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	5.0	5.0
IEEE 802.3X Pause frame transmit For more information, see Features in release 5.3 on page 13.	N/A	5.3
Link Layer Discovery Protocol (LLDP) For more information, see Features in release 5.3 on page 13.	N/A	5.3
Media Access Control Security (MACsec) ✱ **Note:** VOSS 5.0 officially removes the replay protection commands. Do not use replay protection in earlier releases. For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.1	4.2

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
Microsoft Network Load Balancing Service (NLBS) • Unicast mode For more information, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-500.	4.0	4.2
MultiLink Trunking (MLT) / Link Aggregation Group (LAG) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on VSP Operating System Software*, NN47227-503.	4.0	4.2
Spanning Tree Protocol (STP) • Multiple Spanning Tree Protocol (MSTP) • Rapid Spanning Tree Protocol (RSTP) For more information, see the following documents: • *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 4000 Series*, NN46251-500 • *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-500	4.0	4.2
Avaya Fabric technologies		
All Fabric Connect services with Avaya switch cluster For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.0	4.2
Equal Cost Trees (ECT) For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.0	4.2
E-Tree and Private VLANs • For more information about E-Tree, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510. • For more information about Private VLANs, see the following documents: - *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 4000 Series*, NN46251-500 - *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-500 • For information about how to configure MultiLink Trunks (MLT) and Private VLANs, see *Configuring Link Aggregation, MLT, SMLT, and vIST on VSP Operating System Software*, NN47227-503.	4.1	4.2
Fabric Attach	5.0	5.0

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.		
Fabric Extend For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	5.0	5.0
Inter-VSN routing For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.0	4.2
IPv6 inter-VSN routing For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.1	4.2
IP Multicast over Fabric Connect For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.1	4.2
IP Shortcut routing including ECMP For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.0	4.2
IPv6 Shortcut routing For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.1	4.2
IS-IS accept policies For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.1	4.2
Layer 2 Virtual Service Network (VSN) For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.0	4.2
Layer 3 VSN For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.1	4.2
`run spbm` installation script For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.1	4.2
`run vms install` script For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	N/A	N/A
Switched UNI	5.0	5.0

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.		
Transparent Port UNI (T-UNI) For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.2.1	4.2.1
Layer 3 IPv4 and IPv6 routing services		
Address Resolution Protocol (ARP) • Proxy ARP • Static ARP For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	4.0	4.2
Alternative Routes for IPv4 For more information, see *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505	4.0	4.2
Alternative Routes for IPv6 For more information, see *Configuring IPv6 Routing on VSP Operating System Software*, NN47227-507	5.1	5.1
Border Gateway Protocol (BGP) for IPv4 For more information, see *Configuring BGP Services on VSP Operating System Software*, NN47227-508.	4.1	4.2
BGP+ (BGP for IPv6) For more information, see *Configuring BGP Services on VSP Operating System Software*, NN47227-508.	5.0	5.0
Internal Border Gateway Protocol (IBGP) For more information, see *Configuring BGP Services on VSP Operating System Software*, NN47227-508.	4.2	4.2
External Border Gateway Protocol (EBGP) For more information, see *Configuring BGP Services on VSP Operating System Software*, NN47227-508.	4.1	4.2
Dynamic Host Configuration Protocol (DHCP) Relay, DHCP Option 82 For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505	4.0	4.2

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
• *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505		
DHCP Snooping and Neighbor Discovery Inspection • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	5.1	5.1
Equal Cost Multiple Path (ECMP) for IPv4 For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	4.0	4.2
Equal Cost Multiple Path (ECMP) for IPv6 For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505 • *Configuring IPv6 Routing on VSP Operating System Software*, NN47227-507 • *Configuring BGP Services on VSP Operating System Software*, NN47227-508 • *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510	5.1	5.1
Gratuitous ARP filtering For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	4.2	4.2
Internet Control Message Protocol (ICMP) For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	4.0	4.2

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
Internet Group Management Protocol (IGMP) , including virtualization For more information, see the following documents: • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series* , NN46251-504 • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-504	4.0.1	4.2
IP route policies For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	4.0	4.2
IPsec for IPv6 For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.2	4.2
IPv6 (OSPFv3, VRRP, RSMLT, DHCP Relay, IPv4 in IPv6 tunnels) For more information, see *Configuring IPv6 Routing on VSP Operating System Software*, NN47227-507.	4.1	4.2
Layer 3 switch cluster (Routed SMLT) with Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on VSP Operating System Software*, NN47227-503.	4.0	4.2
Layer 3 switch cluster (Routed SMLT) with Simplified vIST For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on VSP Operating System Software*, NN47227-503.	4.0.1	4.2
Multicast Listener Discovery For more information, see the following documents: • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series* , NN46251-504 • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-504	5.1	5.1
Multicast Route Statistics for IPv4 and IPv6	5.1	5.1

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-504.		
Open Shortest Path First (OSPF) For more information, see the following documents: • *Configuring OSPF and RIP on Avaya Virtual Services Platform 4000 Series*, NN46251-506 • *Configuring OSPF and RIP on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-506	4.0	4.2
Protocol Independent Multicast over IPv6 For more information, see the following documents: • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series* , NN46251-504 • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-504	5.1	5.1
Protocol Independent Multicast–Sparse Mode (PIM-SM), PIM-Source Specific Mode (PIM-SSM) For more information, see the following documents: • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series* , NN46251-504 • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-504	4.0.1	4.2
Route Information Protocol (RIP) For more information, see the following documents: • *Configuring OSPF and RIP on Avaya Virtual Services Platform 4000 Series*, NN46251-506 • *Configuring OSPF and RIP on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-506	4.0	4.2
RIPng For more information, see *Configuring IPv6 Routing on VSP Operating System Software*, NN47227-507.	5.0	5.0
Static routing For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	4.0	4.2

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
Unicast Reverse Path Forwarding (URPF) checking (IPv4 and IPv6) For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	5.0	5.0
Virtualization with IPv4 Virtual Routing and Forwarding (VRF) • ARP • DHCP Relay • Inter-VRF Routing (static, dynamic, and policy) • Local Routing • OSPFv2 • RIPv1/2 • Route Policies • Static Routing • VRRP For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	4.0	4.2
Virtual Router Redundancy Protocol (VRRP) • Avaya Backup Master For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	4.0	4.2
VRRPv3 for IPv4 and IPv6 For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505 • *Configuring IPv6 Routing on VSP Operating System Software*, NN47227-507	5.1	5.1

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
• *Performance Management of Avaya Virtual Services Platform 4000 Series*, NN46251-701 • *Monitoring Performance on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-701		
Quality of Service and filtering		
Access Control List (ACL)-based filtering • Egress ACLs • Ingress ACLs • Layer 2 to Layer 4 filtering • Port • VLAN For more information, see the following documents: • *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series*, NN46251-502 • *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-502	4.0	4.2
Avaya Auto QoS For more information, see the following documents: • *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series*, NN46251-502 • *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-502	4.0	4.2
Differentiated Services (DiffServ) including Per-Hop Behavior For more information, see the following documents: • *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series*, NN46251-502 • *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-502	4.0	4.2
Egress port shaper For more information, see the following documents: • *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series*, NN46251-502 • *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-502	4.0	4.2
IPv6 ACL filters	4.1	4.2

Table continues…

Features	Release by platform series	
	VSP 8200	VSP 8400
For more information, see the following documents: • *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series*, NN46251-502 • *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-502		
QoS ingress port rate limiter For more information, see the following documents: • *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series*, NN46251-502 • *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-502	4.0	4.2