Release Notes for Avaya Virtual Services Platform 4000 Series and 8000 Series

Release 4.2
NN47227-401
Issue 05.02
May 2015

© 2015 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, 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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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: http://support.avaya.com 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You 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.

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: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://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: http://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, 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 describes important information about this release for the following families of Avaya Ethernet switches:

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

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.

Related resources

Documentation

See *Documentation Roadmap for Avaya Virtual Services Platform 4000 Series,* NN46251-100 and *Documentation Reference for Avaya Virtual Services Platform 8000 Series*, NN47227-100 for a list of the documentation for these products.

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.

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.

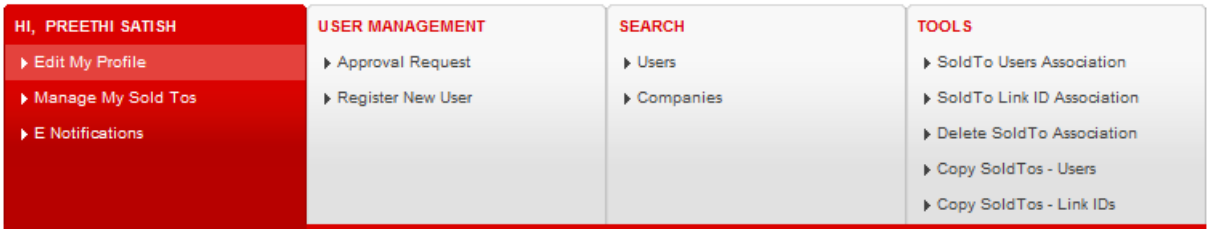
About this task

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 8800.

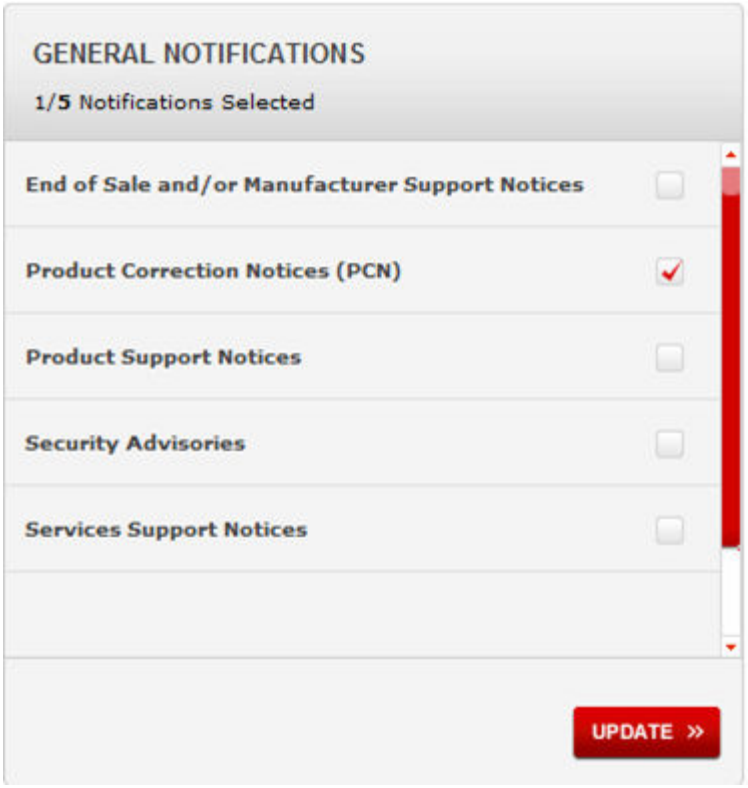
Procedure

1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Click **MY PROFILE**.

4. On the site toolbar, click your name, and then click **E Notifications**.

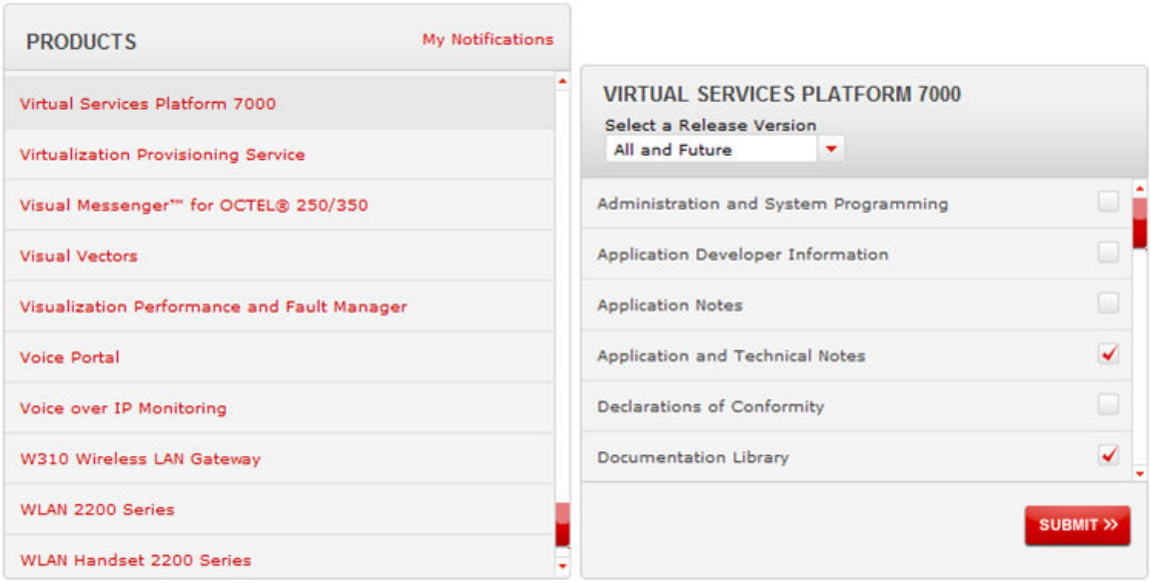


5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.



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

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.



11. Click **Submit**.

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.

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.

Chapter 2: New in this release

The following sections detail what is new in *Release Notes for Avaya Virtual Services Platform 4000 Series and 8000 Series*, NN47227-401 for Release 4.2.

Features

See the following sections for information about feature changes.

New hardware

Release 4.2 introduces the following new hardware:

- VSP 8400 switch, which supports the following four Ethernet Switch Modules (ESMs):
  - 8424XS: 24-port 10GBASE-SFP+ ESM
  - 8424XT: 24-port 10GBASE-T ESM
  - 8408QQ: 8-port* 40GBASE-QSFP+ ESM
  - 8418XSQ: 16-port 10GBASE-SFP+ and 2-port 40GBASE-QSFP+ Combo ESM

    For details on the VSP 8400 hardware and ESMs, see Hardware compatibility for VSP 8000 Series on page 46 and *Installing the Avaya Virtual Services Platform 8000 Series*, NN47227-300.
- New QSFP+ direct attach cables:
  - QSFP+ to QSFP+ 40–gigabit, 0.5 meter Direct Attach Cable (DAC) assembly, which directly connects two QSFP+ ports
  - QSFP+ to four SFP+ 10–gigabit direct attach breakout cable (BOC) assembly, which directly connect one QSFP+ port to four channelized SFP+ ports

    For details on these two new cables, see *Installing Transceivers and Optical Components on Avaya Virtual Services Platform 8000 Series*, NN47227-301.

Authentication and password enhancements (enhanced secure mode)

Release 4.2 supports authentication and password enhancements. After you enable the new **`boot config flags enhancedsecure-mode`**, enhanced secure mode provides new role-based access levels, stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use.

For more information on system access security enhancements, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600 and *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.

Border Gateway Protocol

Release 4.2 updates the Border Gateway Protocol (BGP) to support the Internal Border Gateway Protocol (iBGP) and External Border Gateway Protocol (eBGP) features.

Note:

iBGP support is for GRT only.

For more information, see *Configuring BGP on Avaya Virtual Services Platform 4000 Series,*and *Configuring BGP Services on Avaya Virtual Services Platform 8000 Series*.

Channelization

Release 4.2 adds support for channelization, which allows you to configure 40Gbps QSFP+ ports to operate as four 10 Gigabit Ethernet ports.

Note that when a 40 Gig port is channelized, you should only use break out cables (DAC or Fiber) in it. Otherwise, the link behavior would be unpredictable because it could result in mismatched link status between link partners, which can further lead to network issues.

You should also avoid the use of break out cables in non-channelized 40 Gigabit ports because this could result in mismatched link status between link partners, which can lead to network issues.

For more information on channelization, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.

Encryption module changes

Release 4.2 includes the encryption modules in the image file. There are no separate encryption modules. Therefore, the command **`load-encryption-module`** has been removed. The commands are no longer required for the current release to load the encryption modules. However, if you downgrade the switch from the Release 4.2 version, you continue to require these commands. For more information, see the procedure, Downgrading the software on page 73.

Gratuitous ARP changes

Release 4.2 adds the ability to enable and disable Gratuitous Address Resolution Protocol (ARP).

For more information on the new **`ip gratuitous-arp`** command, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600 and *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.

Internet Protocol Security (IPsec)

Release 4.2 adds support for Internet Protocol Security (IPSec) for IPv6. IPSec adds support for OSPF virtual link for the security protection of the communication between the end points. You can also use IPSec with OSPFv3 on a brouter port or VLAN interface, for example, if you want to encrypt OSPFv3 control traffic on a broadcast network. You can also use IPSec with ICMPv6.

For more information on IPsec for IPv6, see *Security for Avaya Virtual Services Platform 4000 Series,* NN46251-601 and *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601, and *Configuring IPv6 Routing on Avaya Virtual Services Platform 4000 Series and 8000 Series*, NN47227–507.

Log file updates with enhanced secure mode

With enhanced secure mode enabled, only individuals in the administrator or auditor role-based access levels can view log files to analyze switch access and configuration activity. However, no

access level role can modify the content of the log files, not even the administrator or the auditor access level roles. After you enable enhanced secure mode, you cannot delete or clear log files no matter what your role-based access level is.

If you enable enhanced secure mode, you cannot access the following commands for log files at any role-based access level:

- **more**
- **edit**
- **move**
- **rename**
- **copy**
- **remove**

If someone attempts to access a log file with the preceding commands an information and warning message displays on the screen.

After you enable enhanced secure mode, authorized users can use SFTP to transfer files to a remote server with contents encrypted.

If you enable enhanced secure mode, the system encrypts the entire log file.

For more information on log files, see: *Troubleshooting of Avaya Virtual Services Platform 4000 Series,* NN46251-700, *Fault Management of Avaya Virtual Services Platform 4000 Series,* NN46251-702, *Troubleshooting Avaya Virtual Services Platform 8000 Series*, NN47227-700, and *Managing Faults on Avaya Virtual Services Platform 8000 Series*, NN47227-702.

Remote Monitoring 2 (RMON2)

Release 4.2 adds support for Remote Monitoring 2 (RMON2) and updates information about RMON1.

Remote Monitoring (RMON) is a management information base (MIB) or a group of management objects that you use to obtain or configure values using the Simple Network Management Protocol (SNMP). Remote Monitoring 1 (RMON1) is the original version of the protocol, which collects information for OSI Layer 1 and Layer 2 in Ethernet networks. RMON1 provides traffic statistics at the MAC layer, and provides statistics on Ethernet segments for packets and bytes received and transmitted.

RMON2 monitors network and application layer protocols on configured network hosts that you enable for monitoring. RMON2 expands the capacity of RMON1 to upper layer protocols in the OSI model. RMON2 adds the following MIBS: protocol directory, protocol distribution, address map, network-layer host and application layer host for the traffic passing through the CP for these MIB tables.

The system only collects statistics for packets that pass through the Control Processor (CP). RMON2 does not monitor packets on other interfaces processed on the switch that do not pass through the Control Processor (CP).

RMON2 collects statistics on:

- Protocols predefined by the system.
- Address mapping between physical and network address on particular network hosts that you configure for monitoring.

- Network host statistics for particular hosts on a network layer protocol (IP) that you configure for monitoring.
- Application host statistics for particular host on an application layer protocol that you configure for monitoring.

For more information on RMON2, see *Performance Management of Avaya Virtual Services Platform 4000 Series,* NN46251-701, *Fault Management of Avaya Virtual Services Platform 4000 Series,* NN46251-702, *Monitoring Performance on Avaya Virtual Services Platform 8000 Series*, NN47227-701, and *Managing Faults on Avaya Virtual Services Platform 8000 Series*, NN47227-702.

Russia summer time zone changes

According to a recent bill passed by the government of Russia, from October 2014 Moscow has moved from UTC+4 into UTC+3 time zone with no daylight savings. Accurate time configuration is important for security, authentication and logging functions of Avaya solutions.

For more information on time zone configuration, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600 and *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.

SNMP Q-Bridge MIB support

Release 4.2 adds support to Q-Bridge MIB (Management Information Base) which is an industry standard to get statistics from switches.

For more information on Q-Bridge MIB, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600and *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.

Secure Copy changes

The current release does not support Secure Copy (SCP). The preferred alternative file transfer mechanism is Secure File Transfer Protocol (SFTP). A secondary alternative is File Transfer Protocol (FTP).

This feature change has impact on the following areas:

- **Scripts:** For those scripts that use SCP for file transfer, they will need to be modified to use SFTP or FTP in place of SCP.
- **Third-party tools:** For those tools that currently use SCP, the alternate methods of support are SFTP or FTP.
- **COM:** Because COM does not support SFTP, the alternative file transfer mechanism in place of SCP is to enable and use FTP.

  To enable FTP support in COM, do the following:

  Within COM, under the Admin Group, modify the Device Credentials for the devices. In the Device and Server Credentials Editor, edit the Credential Set; click on the FTP tab and populate the FTP User field and Password field that match with the devices. Save the changes, and then, you will be able to use FTP in COM with the devices.

  For more information on COM, see the COM documentation.

For more information on this feature change, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600, *Quick Start for Avaya Virtual Services Platform 4000 Series,*

NN46251-102, *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600, and *Quick Start Configuration for Avaya Virtual Services Platform 8000 Series*, NN47227-102.

Secure hash algorithm 1 and secure hash algorithm 2

Release 4.2 adds support for the secure hash algorithm 1 (SHA-1) and SHA-2.

SHA-1 is a cryptographic hash function that uses 160-bit encryption, usually given in a 40 digit hexadecimal number. SHA-1 is one of the most widely used of the existing SHA hash functions and is more secure than MD5.

SHA-2 is also a cryptographic hash function. SHA-2 updates SHA-1 and offers six hash functions that include SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA 512/256, with hash values that are 224, 256, 384, or 512 bits message digest size values. Output size depends on the hash function, so, for instance SHA-256 is 256 bits.

SHA-1 and SHA-2 take a variable length input message and create a fixed length output message referred to as the hash, or message digest, of the original message. If you use SHA-1 or SHA-2 with OSPF, each OSPF packet has a message digest appended to it. The message digest or hash must match between the sending and receiving routers. If the message digest computed at the sender and receiver does not match, the receiver rejects the packet. The hash functions produce a type of checksum or summary of the input.

For more information, see *Configuring OSPF and RIP on Avaya Virtual Services Platform 8000 Series* , NN47227-506 or *Configuring OSPF and RIP on Avaya Virtual Services Platform 4000 Series,* NN46251–506.

Secure Shell changes

Release 4.2 updates Secure Shell implementation on the switch. The switch now supports only Secure Shell version 2 (SSHv2).

SSHv2 also adds encryption support for MD5, SHA-1.

For more information, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600 and *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.

SNMPv3 enhancements

Release 4.2 updates SNMPv3 to support Federal Information Processing Standards (FIPS) 140-2. SNMPv3 supports the Advanced Encryption Standard (AES) and Data Encryption Standard (DES) encryption options and Message Digest algorithm 5 (MD5), and Secure Hash Algorithm 1 (SHA-1).

If you enable enhanced secure mode, the VSP switch does not support the default SNMPv1 and default SNMPv2 community strings, and default SNMPv3 user name. The individual in the administrator access level role can configure a non-default value for the community strings, and the VSP switch can continue to support SNMPv1 and SNMPv2. The individual in the administrator access level role can also configure a non-default value for the SNMPv3 user name and the VSP switch can continue to support SNMPv3.

If you disable enhanced secure mode, the SNMPv1 and SNMPv2 support for community strings remains the same, and the default SNMPv3 user name remains the same. Enhanced secure mode is disabled by default.

For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601 and *Security for Avaya Virtual Services Platform 4000 Series,* NN46251-601.

SoNMP Changes

Release 4.2 updates the SoNMP Topology Discovery Protocol to include support for channelization. The SONMP hello packet includes sub-port information channelization is enabled.

Overview of features and hardware models by release for the VSP 4000

This section provides an overview of the software features and hardware models introduced in Releases 4.2, 4.1, 4.0, 3.1.0.2, 3.1, 3.0.1, and 3.0 for the Virtual Services Platform 4000.

Note:

No new software features are introduced in release 4.0.40 and 4.0.50.

Features for Releases 4.2, 4.1, 4.0, 3.1.0.2, 3.1, 3.0.1, and 3.0

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

Features	New in this release				
	3.0.X	3.1	4.0	4.1	4.2
Operations and Management					
Authentication and password enhancements For more information, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600.					X
Avaya CLI (ACLI) For more information, see *Commands Reference for Avaya Virtual Services Platform 4000 Series,* NN46251-104.	X				
Encryption modules file included in the Runtime Software Image file The encryption modules file is no longer a separate fie. The encryption modules are included in the Runtime Software Image file.					X
Enterprise Device Manager (EDM) For more information, see Avaya Configuration and Orchestration Manager (COM) documentation, http://support.avaya.com.	X				
Extensible Authentication Protocol over LAN (EAPoL) For more information, see *Security for Avaya Virtual Services Platform 4000 Series,* NN46251-601.					
Flight Recorder for system health monitoring For more information, see *Troubleshooting of Avaya Virtual Services Platform 4000 Series,* NN46251-700.	X				

Table continues…

Features	New in this release				
	3.0.X	3.1	4.0	4.1	4.2
FTP Server For more information, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600.	X				
HTTP and HTTPS EDM management For more information, see *User Interface Fundamentals for Avaya Virtual Services Platform 4000 Series,* NN46251-103.	X				
IEEE 802.1ag Connectivity Fault Management (CFM) For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series,* NN46251-510.	X				
IEEE 802.1ax (802.3ad) Link Aggregation Control Protocol (LACP) For more information, see *Configuring Link Aggregation and MLT on Avaya Virtual Services Platform 4000 Series,* NN46251-503.	X				
Key Health Indicator (KHI) For more information, see *Fault Management of Avaya Virtual Services Platform 4000 Series,* NN46251-702.	X				
Media Access Control Security (MACsec) For more information, see *Security for Avaya Virtual Services Platform 4000 Series,* NN46251-601. **Note:** The MACsec feature is not supported on the VSP 4450GTX-HT-PWR+.			X		
RADIUS For more information, see *Security for Avaya Virtual Services Platform 4000 Series,* NN46251-601.	X				
Remote Monitoring 1 (RMON1) for Layer 1 and Layer 2 For more information, see *Performance Management of Avaya Virtual Services Platform 4000 Series,* NN46251-701 and *Fault Management of Avaya Virtual Services Platform 4000 Series,* NN46251-702.			X		
Remote Monitoring 2 (RMON2) for network and application layer protocols For more information, see *Performance Management of Avaya Virtual Services Platform 4000 Series,* NN46251-701 and *Fault Management of Avaya Virtual Services Platform 4000 Series,* NN46251-702.					X
Russia summer time zone change For more information, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600.					X
Secure Shell and Secure Copy Server	X				

Table continues…

Features	New in this release				
	3.0.X	3.1	4.0	4.1	4.2
Note: The current release does not support SCP. For more information, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600.					
Secure hash algorithm 1 (SHA-1) and SHA-2 For more information, see *Configuring OSPF and RIP on Avaya Virtual Services Platform 4000 Series,* NN46251–506.					X
Secure Shell changes For more information, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600.					X
Secure Sockets Layer (SSL) certificate management For more information, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600				X	
Simple Loop Prevention Protocol (SLPP) For more information, see *Network Design Reference for Avaya Virtual Services Platform 4000 Series,* NN46251–200.	X				
SLPP Re-Arm For more information, see *Network Design Reference for Avaya Virtual Services Platform 4000 Series,* NN46251–200.	X				
Simple Network Management Protocol (SNMP) For more information, see *Security for Avaya Virtual Services Platform 4000 Series,* NN46251-601.	X				
`spbm-config-mode` boot flag For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series* , NN46251–504.				X	
TACACS+ For more information, see *Security for Avaya Virtual Services Platform 4000 Series,* NN46251-601.			X		
Telnet client and server For more information, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600.	X				
TFTP Client and Server For more information, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600.	X				
Virtual LACP (VLACP) End-to-End connectivity check	X				

Table continues…

Features	New in this release				
	3.0.X	3.1	4.0	4.1	4.2
For more information, see *Configuring Link Aggregation and MLT on Avaya Virtual Services Platform 4000 Series,* NN46251-503.					
9k Jumbo packet support For more information, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600.	X				
Layer 2					
Avaya VENA Switch Cluster (Multi-Chassis LAG) • Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation and MLT on Avaya Virtual Services Platform 4000 Series,* NN46251-503.				X	
IEEE 802.1d Mac Bridges Spanning Tree For more information, see *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 4000 Series,* NN46251-500.	X				
IEEE 802.1s MSTP For more information, see *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 4000 Series,* NN46251-500.	X				
IEEE 802.1w RSTP For more information, see *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 4000 Series,* NN46251-500.	X				
MLT (Multilink trunking) For more information, see *Configuring Link Aggregation and MLT on Avaya Virtual Services Platform 4000 Series,* NN46251-503.	X				
Avaya VENA Fabric Connect					
Customer VLAN UNI with Avaya VENA Switch Cluster For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series,* NN46251-510.				X	
IS-IS accept policies. For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series,* NN46251-510.				X	
IP Multicast over Fabric Connect For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series,* NN46251-510.		X			
Transparent UNI (T-UNI) For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series,* NN46251-510.		X			
ETree configuration	X				

Table continues…

Features	New in this release				
	3.0.X	3.1	4.0	4.1	4.2
For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series,* NN46251-510.					
IEEE 802.1aq Shortest Path Bridging MAC-in-MAC (SPBM) For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series,* NN46251-510.	X				
Inter-VSN Routing For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series,* NN46251-510.	X				
Layer 3 IPv4 and IPv6 Routing Services					
L3 Switch Cluster (Routed SMLT) with Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation and MLT on Avaya Virtual Services Platform 4000 Series,* NN46251-503.				X	
L3 Switch Cluster (Routed SMLT) with Simplified vIST For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series* , NN46251–504.				X	
Protocol Independent Multicast–Sparse Mode (PIM-SM), PIM-Source Specific Mode (PIM-SSM) For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series* , NN46251–504				X	
Autogenerated CFM MEP and MIP levels For more information, see *Configuring OSPF and RIP on Avaya Virtual Services Platform 4000 Series,* NN46251–506.		X			
BGP services For more information, see *Configuring BGP on Avaya Virtual Services Platform 4000 Series,* NN46251–507.		X			
Internal Border Gateway Protocol For more information, see *Configuring BGP on Avaya Virtual Services Platform 4000 Series,* NN46251–507.					X
External Border Gateway Protcol For more information, see *Configuring BGP on Avaya Virtual Services Platform 4000 Series,* NN46251–507.					
OSPF and RIP For more information, see *Configuring OSPF and RIP on Avaya Virtual Services Platform 4000 Series,* NN46251–506.		X			
ARP and RARP For more information, see *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series,* NN46251-505.	X				

Table continues…

Features	New in this release				
	3.0.X	3.1	4.0	4.1	4.2
Gratuitous ARP enhancements For more information, see *Administration for Avaya Virtual Services Platform 4000 Series,*					X
DHCP Relay agent For more information, see *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series,* NN46251-505.	X				
DHCP Relay Option 82 For more information, see *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series,* NN46251-505.	X				
Equal Cost MultiPath (ECMP) For more information, see *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series,* NN46251-505.	X				
IP Static routes For more information, see *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series,* NN46251-505.	X				
IPsec for IPv6 For more information, see *Security for Avaya Virtual Services Platform 4000 Series,* NN46251-601.					X
Microsoft NLB ARP multicast-MAC-flooding support For more information, see *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series,* NN46251-505.	X				
Virtual Router Redundancy Protocol (VRRP) For more information, see *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series,* NN46251-505.	X				
Virtual Routing Forwarding (VRF) Lite (24 instances) For more information, see *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series,* NN46251-505.	X				
VRRP BackupMaster For more information, see *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series,* NN46251-505.	X				
Quality-of-Service and filtering					
Service Level Agreement Monitor For more information, see *Performance Management of Avaya Virtual Services Platform 4000 Series,* NN46251-701.			X		
Private VLAN	X				

Table continues…

Features	New in this release				
	3.0.X	3.1	4.0	4.1	4.2
For more information, see *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 4000 Series,* NN46251-500.					
Diffserv framework For more information, see *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series,* NN46251-502.	X				
Egress port shapers For more information, see *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series,* NN46251-502.	X				
IEEE 802.1p/q Virtual LAN For more information, see *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 4000 Series,* NN46251-500.	X				
Ingress port policers For more information, see *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series,* NN46251-502.	X				
IP Brouter port For more information, see *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 4000 Series,* NN46251-500.	X				
Line Rate Ingress and Egress Port and VLAN ACLs for L2 to L4 For more information, see *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series,* NN46251-502.	X				
Port and Protocol-based VLANs For more information, see *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 4000 Series,* NN46251-500.	X				
Port Mirroring ingress and egress For more information, see *Troubleshooting of Avaya Virtual Services Platform 4000 Series,* NN46251-700.	X				

Hardware models for Releases 4.0.50, 4.0.40, 4.0, and 3.x

The following table provides a listing of the hardware models introduced in Virtual Services Platform 4000 Releases 4.0.50, 4.0.40, 4.0, and 3.x.

Model	Part number	Release
VSP 4450GSX-DC	EC4400004–E6	4.0.50
TAA-compliant VSP 4450GSX-PWR+	EC4400A05-E6GS EC4400E05-E6GS	4.0.50
VSP 4450GTX-HT-PWR+	EC4400A03-E6 EC4400E03-E6	4.0.40

Table continues…

Model	Part number	Release
VSP 4450GSX-PWR+	EC4400x05-E6 **Note:** Replace the “x” with a country-specific power cord code listed in VSP 4000 power supplies on page 52.	4.x
VSP 4850GTS	EC4800x78-E6 **Note:** Replace the “x” with a country-specific power cord code listed in VSP 4000 power supplies on page 52.	3.x
VSP 4850GTS-PWR+	EC4800x88-E6 **Note:** Replace the “x” with a country-specific power cord code listed in VSP 4000 power supplies on page 52.	3.x
VSP 4850GTS DC	EC4800078-E6	3.x

For more information about hardware models, see Hardware compatibility on page 50, and *Installing Avaya Virtual Services Platform4450GTX-HT-PWR+Switch, NN46251–304* and *Installing Avaya Virtual Services Platform4450GSX-PWR+Switch, NN46251–307*.

Overview of features and hardware models by release for the VSP 8200

This section provides an overview of the software features and hardware introduced in Releases 4.0.x, 4.1, and 4.2 for the Virtual Services Platform 8200. For subsequent releases, the following table will expand to list new software features.

Note:

Each release includes all the features from previous releases unless specifically stated otherwise.

Features for Releases 4.0.x, 4.1, and 4.2

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

Features	New in this release			
	4.0	4.0.1	4.1	4.2
Operations and Management				
Authentication and password enhancements For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.				X
Avaya CLI (ACLI) For more information, see *ACLI Commands Reference for Avaya Virtual Services Platform 8000 Series*, NN47227-104.	X			
Channelization For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.				X
Configuration and Orchestration Manager (COM) For more information, see Avaya Configuration and Orchestration Manager (COM) documentation, http://support.avaya.com/.	X			
Domain Name Service (DNS) client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X			
Domain Name Service (DNS) client (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.			X	
Encryption modules file included in the Runtime Software Image file The encryption modules file is no longer a separate fie. The encryption modules are included in the Runtime Software Image file.				X
Enterprise Device Manager (EDM) For more information, see *Using ACLI and EDM on Avaya Virtual Services Platform 8000 Series*, NN47227-103.	X			
Etree and Private VLANs • For more information about Etree, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510. • For more information about private VLANs, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 8000 Series*, NN47227-500 . • For information about configuring MultiLink Trunks (MLT) and Private VLANs, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8000 Series*, NN47227-503.			X	

Table continues…

Features	New in this release			
	4.0	4.0.1	4.1	4.2
File Transfer Protocol (FTP) server/client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X			
File Transfer Protocol (FTP) server/client (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.			X	
Flight Recorder (for system health monitoring) For more information, see *Troubleshooting Avaya Virtual Services Platform 8000 Series*, NN47227-700.	X			
IEEE 802.1ag Connectivity Fault Management (CFM) • L2 Ping • TraceRoute • TraceTree For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X			
802.1x-2001 Extended Authentication Protocol (EAP) and EAP over LAN (EAPoL)			X	
Key Health Indicator (KHI) For more information, see *Managing Faults on Avaya Virtual Services Platform 8000 Series*, NN47227-702.	X			
Logging (log to file and syslog [IPv4]) For more information, see *Managing Faults on Avaya Virtual Services Platform 8000 Series*, NN47227-702.	X			
Logging (log to file and syslog [IPv6]) For more information, see *Managing Faults on Avaya Virtual Services Platform 8000 Series*, NN47227-702.			X	
Mirroring (port and flow-based) For more information, see *Troubleshooting Avaya Virtual Services Platform 8000 Series*, NN47227-700.	X			
Network Time Protocol (NTP) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X			
Remote Monitoring 1 (RMON1) for Layer 1 and Layer 2 For more information, see *Monitoring Performance on Avaya Virtual Services Platform 8000 Series*, NN47227-701.				

Table continues…

Features	New in this release			
	4.0	4.0.1	4.1	4.2
Remote Monitoring 2 (RMON2) for network and application layer protocols For more information, see *Monitoring Performance on Avaya Virtual Services Platform 8000 Series*, NN47227-701, and *Managing Faults on Avaya Virtual Services Platform 8000 Series*, NN47227-702.				X
RADIUS, Community-based Users (IPv4) For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601.	X			
RADIUS (IPv6) For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601.			X	
Remote Login (Rlogin) server/client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X			
Remote Login (Rlogin) server (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.			X	
Remote Shell (RSH) Server/Client For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X			
Russia summer time zone change For more information, see , *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.				X
Secure Copy (SCP) **Note:** The current release does not support SCP. For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X			
Secure hash algorithm 1 (SHA-1) and SHA-2 For more information, see *Configuring OSPF and RIP on Avaya Virtual Services Platform 8000 Series* , NN47227-506.				X
Secure Shell changes For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.				X
SSH server (IPv6)			X	

Table continues…

Features	New in this release			
	4.0	4.0.1	4.1	4.2
For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.				
SLA Mon™ For more information, see *Monitoring Performance on Avaya Virtual Services Platform 8000 Series*, NN47227-701.			X	
Simple Loop Prevention Protocol (SLPP) For more information, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 8000 Series*, NN47227-500.	X			
Simple Network Management Protocol (SNMP) v1/2/3 (IPv4) For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601.	X			
SNMP (IPv6) For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601.			X	
SoNMP (Avaya topology discovery protocol) For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601.	X			
`spbm-config-mode` boot flag For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8000 Series*, NN47227-504.		X		
TACACS+ For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601.			X	
Telnet server/client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X			
Telnet server/client (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.			X	
Trivial File Transfer Protocol (TFTP) server/client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X			
Trivial File Transfer Protocol (TFTP) server/client (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.			X	

Table continues…

Features	New in this release			
	4.0	4.0.1	4.1	4.2
Virtual Link Aggregation Control Protocol (VLACP) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8000 Series*, NN47227-503.	X			
Layer 2				
Avaya VENA Switch Cluster (Multi-Chassis LAG) • Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8000 Series*, NN47227-503.	X			
Media Access Control Security (MACsec) For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601.			X	
Microsoft Network Load Balancing Service (NLBS) • Unicast mode For more information, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 8000 Series*, NN47227-500.	X			
MultiLink Trunking (MLT) / Link Aggregation Group (LAG) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8000 Series*, NN47227-503.	X			
Spanning Tree Protocol (STP) • Multiple Spanning Tree Protocol (MSTP) • Rapid Spanning Tree Protocol (RSTP) For more information, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 8000 Series*, NN47227-500.	X			
Avaya VENA Fabric Connect				
Customer VLAN UNI with Avaya VENA Switch Cluster For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X			
Equal Cost Trees (ECT) For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X			
Inter-VSN Routing	X			

Table continues…

Features	New in this release			
	4.0	4.0.1	4.1	4.2
For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.				
IPv6 Inter-VSN Routing For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.			X	
IP Multicast over Fabric Connect For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.			X	
IP Shortcut Routing including ECMP For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X			
IPv6 Shortcut Routing For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.			X	
IS-IS accept policies For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.			X	
Layer 2 Virtual Service Network (VSN) For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X			
Layer 3 VSN For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.			X	
`run spbm` installation script For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.			X	
Layer 3 IPv4 and IPv6 Routing Services				
Address Resolution Protocol (ARP) • Proxy ARP • Static ARP For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.	X			
Border Gateway Protocol (BGP) for IPv4 For more information, see *Configuring BGP Services on Avaya Virtual Services Platform 8000 Series*, NN47227–508.			X	
Internal Border Gateway Protocol (iBGP)				X

Table continues…

Features	New in this release			
	4.0	4.0.1	4.1	4.2
For more information, see *Configuring BGP Services on Avaya Virtual Services Platform 8000 Series*, NN47227–508.				
External Border Gateway Protocol (EBGP) For more information, see *Configuring BGP Services on Avaya Virtual Services Platform 8000 Series*, NN47227–508.			X	
Dynamic Host Configuration Protocol (DHCP) Relay, DHCP Option 82 For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.	X			
Equal Cost Multiple Path (ECMP) For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.	X			
Gratuitous ARP enhancements For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600				X
Internet Control Message Protocol (ICMP) For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.	X			
Internet Group Management Protocol (IGMP) , including virtualization For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8000 Series*, NN47227-504.		X		
IP Route Policies For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.	X			
IPsec for IPv6 For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601.	X			
IPv6 (OSPFv3, VRRP, RSMLT, DHCP Relay, IPv4 in IPv6 tunnels) For more information, see *Configuring IPv6 Routing on Avaya Virtual Services Platform 4000 Series and 8000 Series*, NN47227–507.			X	
Layer 3 Switch Cluster (Routed SMLT) with Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8000 Series*, NN47227-503.	X			

Table continues…

Features	New in this release			
	4.0	4.0.1	4.1	4.2
Layer 3 Switch Cluster (Routed SMLT) with Simplified vIST For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8000 Series*, NN47227-504.		X		
Open Shortest Path First (OSPF) For more information, see *Configuring OSPF and RIP on Avaya Virtual Services Platform 8000 Series* , NN47227-506.	X			
Protocol Independent Multicast–Sparse Mode (PIM-SM), PIM-Source Specific Mode (PIM-SSM) For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8000 Series*, NN47227-504.		X		
Route Information Protocol (RIP) For more information, see *Configuring OSPF and RIP on Avaya Virtual Services Platform 8000 Series* , NN47227-506.	X			
Static Routing For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.	X			
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 *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.	X			
Virtual Router Redundancy Protocol (VRRP) • Avaya Backup Master For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.	X			
Quality-of-Service and Filtering				

Table continues…

Features	New in this release			
	4.0	4.0.1	4.1	4.2
Access Control List (ACL)-based filtering • Egress ACLs • Ingress ACLs • Layer 2–Layer 4 Filtering • Port • VLAN For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8000 Series*, NN47227-502.	X			
Access Control List (ACL)-based filtering • Egress ACLs • Ingress ACLs • Layer 2–Layer 4 Filtering • Port • VLAN For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8000 Series*, NN47227-502.	X			
IPv6 ACL filters For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8000 Series*, NN47227-502.			X	
Avaya Auto QoS For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8000 Series*, NN47227-502.	X			
Differentiated Services (DiffServ) including Per-Hop Behavior For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8000 Series*, NN47227-502.	X			
Egress Port Shaper For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8000 Series*, NN47227-502.	X			
Layer 2–Layer 4 Ingress Port Rate Limiter	X			

Table continues…

Features	New in this release			
	4.0	4.0.1	4.1	4.2
For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8000 Series*, NN47227-502.				

VSP 8200 Series hardware models

The following table provides a listing of the hardware models introduced in the Virtual Services Platform 8200 Series.

Model	Part number	Release
VSP 8284XSQ-AC (AC power supply)	EC8200x01-E6 **Note:** Replace the “x” with a country-specific power cord code listed in Hardware compatibility on page 46.	4.0
VSP 8284XSQ AC PS No PC GSA (TAA-compliant; no power cord)	EC8200A01-E6GS	4.0.50.0
VSP 8284XSQ AC PS NA PC GSA (TAA-compliant; North American power cord)	EC8200E01-E6GS	4.0.50.0

For more information about hardware, see Hardware compatibility on page 46, and *Installing the Avaya Virtual Services Platform 8000 Series*, NN47227-300.

Overview of features and hardware models by release for the VSP 8400

This section provides an overview of the software features and hardware introduced in Release 4.2 for the Virtual Services Platform 8400. For subsequent releases, the following table will expand to list new software features.

Note:

Each release includes all the features from previous releases unless specifically stated otherwise.

Features for Release 4.2

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

Features	New in this release				
	4.2				
Operations and Management					
100/1G/10G RJ45 port LED indicators For more information, see *Installing the Avaya Virtual Services Platform 8000 Series*, NN47227-300.	X				
Authentication and password enhancements For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
Avaya CLI (ACLI) For more information, see *ACLI Commands Reference for Avaya Virtual Services Platform 8000 Series*, NN47227-104.	X				
Channelization For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
Configuration and Orchestration Manager (COM) For more information, see Avaya Configuration and Orchestration Manager (COM) documentation, http://support.avaya.com/.	X				
Domain Name Service (DNS) client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
Domain Name Service (DNS) client (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
Encryption modules file included in the Runtime Software Image file The encryption modules file is no longer a separate fie. The encryption modules are included in the Runtime Software Image file.	X				
Enterprise Device Manager (EDM) For more information, see *Using ACLI and EDM on Avaya Virtual Services Platform 8000 Series*, NN47227-103.	X				
EDM representation of physical LED status For more information, see *Installing the Avaya Virtual Services Platform 8000 Series*, NN47227-300	X				

Table continues…

Features	New in this release				
	4.2				
Etree and Private VLANs • For more information about Etree, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510. • For more information about private VLANs, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 8000 Series*, NN47227-500 . • For information about configuring MultiLink Trunks (MLT) and Private VLANs, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8000 Series*, NN47227-503.	X				
File Transfer Protocol (FTP) server/client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
File Transfer Protocol (FTP) server/client (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
Flight Recorder (for system health monitoring) For more information, see *Troubleshooting Avaya Virtual Services Platform 8000 Series*, NN47227-700.	X				
IEEE 802.1ag Connectivity Fault Management (CFM) • L2 Ping • TraceRoute • TraceTree For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X				
802.1x-2001 Extended Authentication Protocol (EAP) and EAP over LAN (EAPoL)	X				
Key Health Indicator (KHI) For more information, see *Managing Faults on Avaya Virtual Services Platform 8000 Series*, NN47227-702.	X				
Logging (log to file and syslog [IPv4]) For more information, see *Managing Faults on Avaya Virtual Services Platform 8000 Series*, NN47227-702.	X				
Logging (log to file and syslog [IPv6])	X				

Table continues…

Features	New in this release				
	4.2				
For more information, see *Managing Faults on Avaya Virtual Services Platform 8000 Series*, NN47227-702.					
Mirroring (port and flow-based) For more information, see *Troubleshooting Avaya Virtual Services Platform 8000 Series*, NN47227-700.	X				
Network Time Protocol (NTP) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
RADIUS, Community-based Users (IPv4) For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601.	X				
RADIUS (IPv6) For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601.	X				
Remote Login (Rlogin) server/client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
Remote Login (Rlogin) server (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
Remote Monitoring 1 (RMON1) for Layer 1 and Layer 2 For more information, see *Monitoring Performance on Avaya Virtual Services Platform 8000 Series*, NN47227-701, and *Managing Faults on Avaya Virtual Services Platform 8000 Series*, NN47227-702.	X				
Remote Monitoring 2 (RMON2) for network and application layer protocols For more information, see *Monitoring Performance on Avaya Virtual Services Platform 8000 Series*, NN47227-701, and *Managing Faults on Avaya Virtual Services Platform 8000 Series*, NN47227-702.	X				
Remote Shell (RSH) Server/Client For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
RMON For more information, see *Monitoring Performance on Avaya Virtual Services Platform 8000 Series*, NN47227-701.	X				
Russia summer time zone change	X				

Table continues…

Features	New in this release				
	4.2				
For more information, see *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600.					
Secure Copy (SCP) **Note:** The current release does not support SCP. For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
Secure hash algorithm 1 (SHA-1) and SHA-2 For more information, see *Configuring OSPF and RIP on Avaya Virtual Services Platform 8000 Series* , NN47227-506.	X				
Secure Shell changes For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
Secure Sockets Layer (SSL) certificate management For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
SSH server (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
SLA Mon™ For more information, see *Monitoring Performance on Avaya Virtual Services Platform 8000 Series*, NN47227-701.	X				
Simple Loop Prevention Protocol (SLPP) For more information, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 8000 Series*, NN47227-500.	X				
Simple Network Management Protocol (SNMP) v1/2/3 (IPv4) For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601.	X				
SNMP (IPv6) For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601.	X				
SoNMP (Avaya topology discovery protocol) For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601.	X				

Table continues…

Features	New in this release				
	4.2				
`spbm-config-mode` boot flag For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8000 Series*, NN47227-504.	X				
TACACS+ For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601.	X				
Telnet server/client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
Telnet server/client (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
Trivial File Transfer Protocol (TFTP) server/client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
Trivial File Transfer Protocol (TFTP) server/client (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
Virtual Link Aggregation Control Protocol (VLACP) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8000 Series*, NN47227-503.	X				
Layer 2					
Avaya VENA Switch Cluster (Multi-Chassis LAG) • Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8000 Series*, NN47227-503.	X				
Media Access Control Security (MACsec) For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.	X				
Microsoft Network Load Balancing Service (NLBS) • Unicast mode For more information, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 8000 Series*, NN47227-500.	X				

Table continues…

Features	New in this release				
	4.2				
MultiLink Trunking (MLT) / Link Aggregation Group (LAG) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8000 Series*, NN47227-503.	X				
Spanning Tree Protocol (STP) • Multiple Spanning Tree Protocol (MSTP) • Rapid Spanning Tree Protocol (RSTP) For more information, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 8000 Series*, NN47227-500.	X				
Avaya VENA Fabric Connect					
Customer VLAN UNI with Avaya VENA Switch Cluster For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X				
Equal Cost Trees (ECT) For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X				
Inter-VSN Routing For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X				
IPv6 Inter-VSN Routing For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X				
IP Multicast over Fabric Connect For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X				
IP Shortcut Routing including ECMP For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X				
IPv6 Shortcut Routing	X				

Table continues…

Features	New in this release				
	4.2				
For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.					
IS-IS accept policies For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X				
Layer 2 Virtual Service Network (VSN) For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X				
Layer 3 VSN For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X				
`run spbm` installation script For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8000 Series*, NN47227-510.	X				
Layer 3 IPv4 and IPv6 Routing Services					
Address Resolution Protocol (ARP) • Proxy ARP • Static ARP For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.	X				
Border Gateway Protocol (BGP) for IPv4 For more information, see *Configuring BGP Services on Avaya Virtual Services Platform 8000 Series*, NN47227–508.	X				
Internal Border Gateway Protocol (iBGP) For more information, see *Configuring BGP Services on Avaya Virtual Services Platform 8000 Series*, NN47227–508.	X				
External Border Gateway Protocol (EBGP) For more information, see *Configuring BGP Services on Avaya Virtual Services Platform 8000 Series*, NN47227–508.	X				
Dynamic Host Configuration Protocol (DHCP) Relay, DHCP Option 82	X				

Table continues…

Features	New in this release				
	4.2				
For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.					
Equal Cost Multiple Path (ECMP) For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.	X				
Gratuitous ARP enhancements For more information, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600	X				
Internet Control Message Protocol (ICMP) For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.	X				
Internet Group Management Protocol (IGMP) , including virtualization For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8000 Series*, NN47227-504.	X				
IP Route Policies For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.	X				
IPsec for IPv6 For more information, see *Configuring Security on Avaya Virtual Services Platform 8000 Series*, NN47227-601.	X				
IPv6 (OSPFv3, VRRP, RSMLT, DHCP Relay, IPv4 in IPv6 tunnels) For more information, see *Configuring IPv6 Routing on Avaya Virtual Services Platform 4000 Series and 8000 Series*, NN47227–507.	X				
Layer 3 Switch Cluster (Routed SMLT) with Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8000 Series*, NN47227-503.	X				
Layer 3 Switch Cluster (Routed SMLT) with Simplified vIST For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8000 Series*, NN47227-504.	X				
Open Shortest Path First (OSPF)	X				

Table continues…

Features	New in this release				
	4.2				
For more information, see *Configuring OSPF and RIP on Avaya Virtual Services Platform 8000 Series* , NN47227-506.					
Protocol Independent Multicast–Sparse Mode (PIM-SM), PIM-Source Specific Mode (PIM-SSM) For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8000 Series*, NN47227-504.	X				
Route Information Protocol (RIP) For more information, see *Configuring OSPF and RIP on Avaya Virtual Services Platform 8000 Series* , NN47227-506.	X				
Static Routing For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.	X				
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 *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.	X				
Virtual Router Redundancy Protocol (VRRP) • Avaya Backup Master For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8000 Series*, NN47227-505.	X				
Quality-of-Service and Filtering					
Access Control List (ACL)-based filtering • Egress ACLs • Ingress ACLs • Layer 2–Layer 4 Filtering • Port • VLAN	X				

Table continues…

Features	New in this release				
	4.2				
For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8000 Series*, NN47227-502.					
Access Control List (ACL)-based filtering • Egress ACLs • Ingress ACLs • Layer 2–Layer 4 Filtering • Port • VLAN For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8000 Series*, NN47227-502.	X				
IPv6 ACL filters For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8000 Series*, NN47227-502.	X				
Avaya Auto QoS For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8000 Series*, NN47227-502.	X				
Differentiated Services (DiffServ) including Per-Hop Behavior For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8000 Series*, NN47227-502.	X				
Egress Port Shaper For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8000 Series*, NN47227-502.	X				
Layer 2–Layer 4 Ingress Port Rate Limiter For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8000 Series*, NN47227-502.	X				

VSP 8400 Series hardware models

The following table provides a list of the hardware models introduced in the Virtual Services Platform 8400 Series.

Table 1: VSP 8404 Hardware

VSP 8404	Part number	Release
VSP 8404–AC This model number ships with one field-replaceable 800 watt **AC** power supply.	EC8400x01-E6 **Note:** Replace the “x” with a country-specific power cord code listed in Hardware compatibility on page 46.	4.2
VSP 8404 AC PS No PC GSA This model number is compliant with the Trade Agreements Act (TAA). It ships with one field-replaceable 800 watt **AC** power supply but no power cord.	EC8400A01-E6GS	4.2
VSP8404 AC PS NA PC GSA This model number is also TAA compliant and ships with an **AC** power supply. However, it includes a North American power cord.	EC8400E01-E6GS	4.2

The following table provides a list of the Ethernet Switch Modules (ESM).

Module	Part number	Release
8408QQ 8 ports of 40GBASE-QSFP+	EC8404003-E6 EC8404003-E6GS (TAA-compliant)	4.2
8418XSQ 6 ports of 10GBASE-SFP+ and 2 ports of 40GBASE-QSFP+	EC8404005-E6 EC8404005-E6GS (TAA-compliant)	4.2
8424XS 4 ports of 10GBASE-SFP+	EC8404001-E6 EC8404001-E6GS (TAA-compliant)	4.2
8424XT 4 ports of 10GBASE-T	EC8404002-E6 EC8404002-E6GS (TAA-compliant)	4.2

For more information about hardware, see Hardware compatibility on page 46, and *Installing the Avaya Virtual Services Platform 8000 Series*, NN47227-300.

VSP 4000 and VSP 8000 feature differences

Avaya has implemented feature parity between the VSP 4000 Series and the VSP 8000 Series in all but a few exceptions. Some features are supported in one platform and not the other to maintain compatibility with previous releases. In other cases, it has to do with the role of the switch in the network.

The following table summarizes the feature differences between the VSP 4000 and VSP 8000 in this release:

Feature	VSP 4000	VSP 8000
40–gigabit Channelization	Not applicable	Supported
CMAC — CFM	Supported	Not Supported
Endura scripts	Supported	Not Supported
FDB protected by port	Supported	Not Supported
NLB Unicast	Not Supported	Supported
QoS	Supported	Supported with exceptions: • Classification does not have routed packet classification • 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
Transparent UNI	Supported	Not Supported

Other changes

The chapter “Supported standards, RFCs, and MIBs” has been removed from this document and moved to the following documents:

- *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600
- *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600

Chapter 3: Important notices

This section describes the supported hardware and software scaling capabilities and provides important information for this release.

Hardware compatibility

This section lists the hardware components for this release.

Hardware compatibility for VSP 8000 Series

This section lists the VSP 8000 Series hardware, which includes the VSP 8200 and the VSP 8400 hardware.

VSP 8200 hardware

Table 2: VSP 8284XSQ Hardware

VSP 8284XSQ	Description	Part number
VSP 8284XSQ-AC This model number ships with one field-replaceable 800 watt **AC** power supply.	• 80 ports of 10GBASE-SFP+ • 4 ports of 40GBASE-QSFP+ • one 10/100/1000BASE-T Out-Of-Band Management Port • one RJ-45 Console Port (10101) • one USB port • Base Software License • four field-replaceable fan modules	EC8200x01-E6 **Note:** Replace the “x” with a country-specific power cord code. See the footnote for details.
VSP 8284XSQ-DC This model number ships with one field-replaceable 800 watt **DC** power supply.	Includes all of the above features.	EC8200001-E6

Table continues…

VSP 8284XSQ	Description	Part number
Note that this model is supported in release 4.0.50.0, but not supported in release 4.2.		
VSP 8284XSQ AC PS No PC GSA This model number is compliant with the Trade Agreements Act (TAA). It ships with one field-replaceable 800 watt **AC** power supply but no power cord.	Includes all of the above features.	EC8200A01-E6GS
VSP 8284XSQ AC PS NA PC GSA This model number is also TAA compliant and ships with an **AC** power supply. However, it includes a North American power cord.	Includes all of the above features.	EC8200E01-E6GS
Redundant power supplies		
800 watt AC redundant power supply	The VSP 8284XSQ comes with one 800 W AC PSU. For full power redundancy, you can install a second 800 W AC PSU.	EC8005x01-E6 **Note:** Replace the “x” with a country-specific power cord code. See the footnote for details.
800 watt DC redundant power supply	The VSP 8284XSQ comes with one 800 W DC PSU. For full power redundancy, you can install a second 800 W DC PSU.	EC8005001-E6
*__Note__: The character (x) in the order number indicates the power cord code. Replace the “x” with the proper letter to indicate desired product nationalization. See the following for details: “A”: No power cord included. “B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden. “C”: Includes power cord commonly used in the United Kingdom and Ireland. “D”: Includes power cord commonly used in Japan. “E”: Includes North American power cord. “F”: Includes Australian power cord.		
Redundant fan trays		

Table continues…

VSP 8284XSQ	Description	Part number
12 volt redundant fan tray	The VSP 8284XSQ comes with all four 12–V fan trays installed.	EC8011004-E6
VSP 8000 Series Universal Slide Rack Mount Kit (300 mm-900 mm) **Note:** The slide rack mount kit is optional and must be ordered separately.		
300 mm–900 mm slide rack mount kit	The VSP 8284XSQ comes with a bracket to install the chassis on a tray. To install the chassis without a tray, install the slide rack mount kit.	EC8011002-E6

VSP 8400 hardware

The following tables describe the VSP 8404 hardware.

Table 3: VSP 8404 Hardware

VSP 8404	Description	Part number
VSP 8404–AC This model number ships with one field-replaceable 800 watt **AC** power supply.	• one 10/100/1000BASE-T Out-Of-Band Management Port • one RJ-45 Console Port • one USB port • Base Software License • four field-replaceable fan modules • No power cord	EC8400x01-E6 **Note:** Replace the “x” with a country-specific power cord code. See the footnote for details.
VSP 8404 AC PS No PC GSA This model number is compliant with the Trade Agreements Act (TAA). It ships with one field-replaceable 800 watt **AC** power supply but no power cord.	Includes all of the above features.	EC8400A01-E6GS
VSP8404 AC PS NA PC GSA This model number is also TAA compliant and ships with an **AC** power supply. However, it includes a North American power cord.	Includes all of the above features.	EC8400E01-E6GS
Redundant power supplies		
800 watt AC redundant power supply	The VSP 8404 comes with one 800 W AC PSU. For full power redundancy, you can install a second 8001-AC-PSU.	EC8005x01-E6

Table continues…

VSP 8404	Description	Part number
	No power cord	
*__Note__: The character (x) in the order number indicates the power cord code. Replace the “x” with the proper letter to indicate desired product nationalization. See the following for details: “A”: No power cord included. “B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden. “C”: Includes power cord commonly used in the United Kingdom and Ireland. “D”: Includes power cord commonly used in Japan. “E”: Includes North American power cord. “F”: Includes Australian power cord.		
Spare fan modules		
Spare fan module	The VSP 8404 comes with all four 12–V fan trays installed. This part can be purchased if a spare fan module is desired.	EC8011004-E6
VSP 8000 Series Universal Slide Rack Mount Kit (300 mm-900 mm) **Note:** The slide rack mount kit is optional and must be ordered separately.		
300 mm–900 mm slide rack mount kit	The VSP 8404 comes with a bracket to install the chassis on a tray. To install the chassis without a tray, install the slide rack mount kit.	EC8011002-E6

Table 4: VSP 8400 Ethernet switch modules (ESMs)

Model Name	Description	Release	Part Number
8424XS	24-port 10GBASE-SFP+ Ethernet Switch Module	4.2.0	EC8404001-E6
8424XS (TAA-compliant)	24-port 10GBASE-SFP+ Ethernet Switch Module	4.2.0	EC8404001-E6GS
8424XT	24-port 10GBASE-T Ethernet Switch Module	4.2.0	EC8404002-E6
8424XT (TAA-compliant)	24-port 10GBASE-T Ethernet Switch Module	4.2.0	EC8404002-E6GS
8408QQ	8-port* 40GBASE-QSFP+ Ethernet Switch Module	4.2.0	EC8404003-E6
8408QQ (TAA-compliant)	8-port* 40GBASE-QSFP+ Ethernet Switch Module	4.2.0	EC8404003-E6GS
8418XSQ	16-port 10GBASE-SFP+ and 2-port 40GBASE-QSFP+ Combo Ethernet Switch Module	4.2.0	EC8404005-E6

Table continues…

Model Name	Description	Release	Part Number
8418XSQ (TAA-compliant)	16-port 10GBASE-SFP+ and 2-port 40GBASE-QSFP+ Combo Ethernet Switch Module	4.2.0	EC8404005-E6GS

Note:

* Two ports are reserved for future use.

Compatible transceivers

Important:

Avaya recommends using Avaya-branded SFP, SFP+, and QSFP+ transceivers as they have been through extensive qualification and testing. Avaya will not be responsible for issues related to non-Avaya branded transceivers.

- The VSP 8000 Series operates in forgiving mode for SFP transceivers, which means that the switch will bring up the port operationally when using non-Avaya SFP transceivers. Avaya does not provide support for operational issues related to these SFPs, but they will operate and the port link will come up. The switch logs the device as an unsupported or unknown device.
- The VSP 8000 Series operates in strict mode for SFP+ and QSFP+ transceivers, which means that the switch will not bring the port up operationally when using non-Avaya SFP+ or QSFP+ transceivers.
- The VSP 8000 Series operates in forgiving mode for SFP+ and QSFP+ direct attached cables, which means that the switch will bring up the port operationally when using Non-Avaya direct attached cables. Avaya does not provide support for operational issues related to these DACs, but they will operate and the port link will come up.

For more information about compatible transceivers, see *Installing Transceivers and Optical Components on Avaya Virtual Services Platform 8000 Series*, NN47227-301.

Hardware compatibility for VSP 4000

The following tables describe the Avaya Virtual Services Platform 4000 Series hardware.

Table 5: Hardware

Release	VSP 4000 model	Description	Part number
3.0	VSP 4850GTS	• 48 10/100/1000 BaseTX RJ-45 ports • two shared SFP ports • two 1/10GE SFP+ ports • Base Software License • one (of two) field replaceable 300W PSUs supplied with the chassis	EC4800x78-E6 **Note:** Replace the “x” with a country-specific power cord code. See

Table continues…

Release	VSP 4000 model	Description	Part number
			the footnote for details.
3.0	VSP 4850GTS-PWR+	• 48 10/100/1000 802.3at PoE+ • two shared SFP ports • two 1/10GE SFP+ ports • Base Software License • one (of two) field replaceable 1000W PSUs supplied with the chassis	EC4800x88-E6 **Note:** Replace the “x” with a country-specific power cord code. See the footnote for details.
3.0	VSP 4850GTS DC	• 48 10/100/1000 Base TX RJ-45 ports • two shared SFP ports • two 1/10GE SFP+ ports • one (of two) field replaceable 300W DC PSUs supplied with the chassis	EC4800078-E6
4.0	VSP 4450GSX-PWR+	• 12 10/100/1000 BASE TX RJ-45 ports with 802.3at PoE+ • 36 100/1000–Mbps SFP ports • Two 1/10G SFP+ ports with MACsec capable PHY • One (of two) field-replaceable 1000W PSUs supplied with the chassis	EC4400x05-E6 **Note:** Replace the “x” with a country-specific power cord code. See the footnote for details.
4.0.40	VSP 4450GTX-HT-PWR+	• 48 10/100/1000 Base TX RJ-45 ports with 802.3at PoE+ • two shared SFP ports • two 1/10GE SFP+ ports • Base Software License • one (of two) field replaceable 1000W PSUs supplied with the chassis	EC4400A03-E6
		• Same content as EC4400A03-E6 with a NA power cord.	EC4400E03-E6
4.0.50	VSP 4450GSX-DC	• 12 10/100/1000 BASE TX RJ-45 ports • 36 100/1000 Mbps SFP ports • two 1/10G SFP+ ports with MACsec capable PHY • one field-replaceable 300W DC PSU	EC4400004-E6

Table continues…

Release	VSP 4000 model	Description	Part number
4.0.50	TAA-compliant VSP 4450GSX-PWR+	• 12 10/100/1000 BASE TX RJ-45 ports with 802.3at PoE+ • 36 100/1000–Mbps SFP ports • Two 1/10G SFP+ ports with MACsec capable PHY • One (of two) field-replaceable 1000W PSUs supplied with the chassis	EC4400x05-E6GS **Note:** Replace the “x” with a country-specific power cord code. See the footnote for details.
Note: The character (x) in the order number indicates the power cord code. Replace the “x” with the proper letter to indicate the desired product nationalization. See the following for details: “A”: No power cord included. “B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden. “C”: Includes power cord commonly used in the United Kingdom and Ireland. “D”: Includes power cord commonly used in Japan. “E”: Includes North American power cord. “F”: Includes Australian power cord.			

VSP 4000 power supplies

The VSP 4000 supports both AC and DC power supplies. One power supply is installed in the system.

You can install a redundant power supply to support additional power requirements or to provide power redundancy.

The following table describes the VSP 4000–compatible AC and DC power supplies and their part numbers (order codes). All the power supplies are EUED RoHS 5/6 compliant.

Note:

The 300–watt and 1000–watt AC power supplies use the IEC 60320 C16 AC power cord connector.

Use the order codes to order a replacement for the primary PSU or to order a redundant PSU for your VSP 4000 system.

Table 6: Power supply order codes

VSP 4000 PSU	Usage	Part number (order code)
300W AC power supply	For use in the ERS 4626GTS, 4850GTS, VSP 4850GTS and WL8180, WL8180-16L wireless controllers.	AL1905?08-E5*

Table continues…

VSP 4000 PSU	Usage	Part number (order code)
Stackable 1000W AC POE+ power supply	For use in 4X00 PWR+.	AL1905?21–E6*
1000W AC PoE+ power supply	For use with VSP 4450GTX-HT-PWR+	EC4005?03–E6
300W DC power supply	For use in the VSP 4850GTS-DC, ERS5698TFD, 5650TD, and 5632FD. DC connector included.	AL1905005-E5

*__Note:__The seventh character (?) of the switch order number must be replaced with the proper letter to indicate desired product nationalization. See the following for details:

“A”: No power cord included.

“B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden.

“C”: Includes power cord commonly used in the United Kingdom and Ireland.

“D”: Includes power cord commonly used in Japan.

“E”: Includes North American power cord.

“F”: Includes Australian power cord.

Important operational note for VSP 4000 switches

This section provides information to take into consideration to prevent system operation failure.

Operational consideration for USB Flash Drive on factory supplied and converted VSP 4000 switches
Warning: The USB FLASH drive on all models of VSP 4850 (factory built and converted from ERS 4850) must be treated as a permanent non-removable part of the switch and must NEVER be removed from the switch to ensure proper operation. Additionally, the USB cover must be installed to ensure additional protection against removal. The USB FLASH drive on the VSP 4850 switch is uniquely and permanently bound to the operating system of the switch it is first used on and cannot be transferred to a different switch. Removal (and reinsertion) of the USB FLASH drive from the switch is not supported as it can permanently compromise the switch functionality and render it non-functional.

Switch conversion

This section lists information on Avaya switch conversion supported in this release.

Important:

Switch conversion is applicable only to the Avaya Virtual Services Platform 4000 Series. Currently, only the conversion of an Avaya ERS 4850 switch to a VSP 4000 switch is supported.

ERS 4850 and VSP 4000 quick conversion

You can convert an Avaya ERS 4850 switch to a VSP 4000 switch, if there is a network requirement. Avaya provides a conversion kit to convert a single installation (not stacked) of an Avaya ERS 4850 switch to a VSP 4000 switch.

The ERS 4850 to VSP 4000 conversion kit (part number EC4810003.3.0) contains:

- VSP 4000 USB FLASH drive with software module (Release 3.0)
- VSP 4000 USB cover
- Stacking port cover and screws
- 60–day trial license for the VSP 4000

USB considerations for factory supplied and converted VSP 4000 switches
Warning: The USB FLASH drive on all models of VSP 4850 (factory built and converted from ERS4850) must be treated as a permanent non-removable part of the switch and must NEVER be removed from the switch to ensure proper operation. Additionally, the USB cover must be installed to ensure additional protection against removal. The USB FLASH drive on the VSP 4850 switch is uniquely and permanently bound to the operating system of the switch it is first used on and cannot be transferred to a different switch. Removal (and reinsertion) of the USB FLASH drive from the switch is not supported as it can permanently compromise the switch functionality and render it non-functional.

On a converted VSP 4000 switch, you can also perform a conversion back to the ERS 4850, using the ACLI.

For the conversion to be successful, you must ensure that the hardware and software criteria on the system being converted, are satisfied. For more information, see *ERS 4850 to VSP 4000 Quick Conversion*, NN46251-400.

Software scaling capabilities

This section lists software scaling capabilities of the Avaya Virtual Services Platform 4000 Series and Avaya Virtual Services Platform 8000 Series.

Table 7: Software scaling capabilities

	Maximum number supported	
	VSP 4000 Series	**VSP 8000 Series**
Layer 2		
MAC Table Size (Without SPBM)	32,000	224,000

Table continues…

	Maximum number supported	
	VSP 4000 Series	**VSP 8000 Series**
MAC Table Size (With SPBM)	16,000	112,000
Port based VLANs	4,059	4,059
Private VLANs (E-Tree)	1,000	4,059
Protocol based VLANs (IPv6 only)	1	1
RSTP Instances	1	1
MSTP Instances	12	12
LACP Aggregators	24	84 (up to 96 with channelization)
Ports per LACP aggregator	16 (8-active, 8-standby)	16 (8-active, 8-standby)
MLT Groups	24	84 (up to 96 with channelization)
Ports per MLT group	8	8
SLPP VLANs	128	128
VLACP Interfaces	50	84 (up to 96 with channelization)
Layer 3 (IPv4 & IPv6 Common)		
IP interfaces (IPv4 or IPv6)	256	506
VRRP interfaces (IPv4/IPv6)	64	252
VRRP Interfaces with fast timers (200ms) - IPv4/IPv6	24	24
ECMP Groups/Paths per group	500/4	1,000/8
OSPF v2/v3 interfaces	48 (24 of these can be passive)	500
OSPF v2/v3 neighbors (adjacencies)	24	500
OSPF Areas	12 for each VRF 64 for the switch	12 for each VRF 80 for the switch
Routed Split Multi-Link Trunking (RSMLT) interfaces (IPv4 or IPv6)	252	252
DHCP Relay forwarding (IPv4 or IPv6)	128	1024
Layer 3 (IPv4)		
IPv4 ARP table	6,000	32,000
IPv4 Static ARP entries	200 for each VRF 1,000 for the switch	2,000 for each VRF 10,000 for the switch
IPv4 CLIP interfaces	64	64
IPv4 Route Table Size	16,000	N/A
IPv4 route table size with "ipv6-mode" boot flag set to false	N/A	16,000

Table continues…

	Maximum number supported	
	VSP 4000 Series	**VSP 8000 Series**
IPv4 route table size with "ipv6-mode" boot flag set to true	N/A	8,000
IPv4 Static Routes	1,000 for each VRF 1,000 for the switch	1,000 per VRF 5,000 for the switch
RIP interfaces	24	200
IPv4 RIP routes	2,000 for each VRF 2,000 for the switch	2,000 for each VRF 2,000 for the switch
IPv4 OSPF routes	16,000 for each VRF 16,000 for the switch	16,000 for each VRF 16,000 for the switch **Note:** The maximum routes supported per VRF is 16,000. The 16,000 routes can be distributed across the 24 VRFs (+ GRT) in any manner.
BGP peers	12	12
IPv4 BGP routes	16,000 for the switch	16,000 for the switch
IPv4 shortcut routes	16,000	16,000
IPv4 Route Policies	500 for each VRF 5,000 for the switch	500 for each VRF 5,000 for the switch
IPv4 NLB Interfaces	N/A	256
IPv4 VRF instances	24	24
IPv4 UDP forwarding	128	512
Layer 3 (IPv6)		
IPv6 Neighbor table	4,000	8,000
IPv6 static neighbor records	128	256
IPv6 CLIP interfaces	1	1
IPv6 route table size (prefix length < 64 bits)	8,000	N/A
IPv6 route table size (prefix length > 64 bits)	256	N/A
IPv6 route table size (Prefix Length < 64 bits) with "ipv6-mode" boot flag set to false	N/A	8,000

Table continues…

	Maximum number supported	
	VSP 4000 Series	**VSP 8000 Series**
IPv6 route table size (Prefix Length > 64 bits) with "ipv6-mode" boot flag set to false	N/A	0
IPv6 route table size (Prefix Length < 64 bits) with "ipv6-mode" boot flag set to true	N/A	4000
IPv6 route table size (Prefix Length > 64 bits) with "ipv6-mode" boot flag set to true	N/A	2000
IPv6 static routes	1,000	1,000
IPv6 OSPFv3 routes - GRT only	8000	8000
IPv6 shortcut routes – GRT only	8,000	8,000
IPv6 6in4 configured tunnels	254	506
IP Multicast		
IGMP interfaces	4,059	4,059
PIM interfaces	128 (Active), 256 (Passive)	128 (Active), 256 (Passive)
PIM Neighbors (GRT Only)	128	128
PIM-SSM static channels	512	4,000
Multicast Receivers or IGMP Joins (per Switch)	1,000	6,000
Multicast senders (per switch)	1,000	6,000
Total Multicast Routes (per Switch)	4,000	6,000
Static Multicast Routes	512	4,000
Multicast enabled Layer 2VSN	1,000	2,000
Multicast enabled Layer 3VSN	24	24
SPBM		
SPBM enabled Switches per region (BEB + BCB)	2,000	2,000
Service endpoint Switches (BEBs) per I-SID	2,000	512
IS-IS interfaces	50	84 (up to 96 with channelization)
IS-IS adjacencies	50	84 (up to 96 with channelization)
Layer 2 VSNs per switch (VLANs mapped to I-SID)	1,000	4,059
Layer 3 VSNs per switch (VRF mapped to I-SID)	24	24

Table continues…

	Maximum number supported	
	VSP 4000 Series	**VSP 8000 Series**
Transparent-UNI services per switch (Port mapped to I-SID)	48	N/A
E-Tree (private VLANs)	1,000	4,059
Filters and QoS		
Total IPv4 Ingress rules/ACEs (Port/VLAN based, Security/QoS filters)	1530	766
Total IPv4 Egress rules/ACEs (Port based, Security filters)	254	252
Total IPv6 Ingress rules/ACEs (Port/VLAN based, Security/QoS filters)	256	256
Diagnostics		
Mirrored ports	49	83 (up to 95 with channelization)
OAM		
FTP sessions (IPv4/IPv6)	4	4
Rlogin sessions (IPv4/IPv6)	8	8
SSH sessions (IPv4/IPv6)	8 total (any combination of IPv4 and IPv6 up to 8)	8 total (any combination of IPv4 and IPv6 up to 8)
Telnet sessions (IPv4/IPv6)	8	8

File names for Release 4.2

This section lists the software files for the following Avaya VSP platforms:

- VSP 4000
- VSP 8200
- VSP 8400

Caution:

To download the software and files, use one of the following browsers: IE 9 or greater, or Mozilla Firefox. Do not use Google Chrome to download software and files.

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 59.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 60. On a Windows machine, use the appropriate Windows utility that is supported on your Windows version.

Note:

Starting in release 4.2, 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: File names and sizes

Product	File name (File size in bytes)		
	Standard Runtime Software Image	EDM Help	MIB Files
VSP 4000 Series	VSP4k.4.2.0.0.tgz (4,165,695)	VSP4000v410_HELP_EDM_gzip.zip (2,773,914)	N/A
VSP 8000 Series	VSP8k.4.2.0.0.tgz (49,500,381)	VOSSv420_HELP_EDM_gzip.zip (2,873,932)	• VSP8k.4.2.0.0_mib.zip (798,496) • VSPk.4.2.0.0_mib.txt (5,163,355)

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 4.2
VSP 4000 Series	VSP4k.4.2.0.0_oss-notice.html	VSP4k.4.2.0.0_OpenSource.zip
VSP 8000 Series	VSP8k.4.2.0.0_oss-notice.html	VSP8k.4.2.0.0_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  VSP8200v4.0.0.0.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
```

Shutting down the system

Use the following procedure to shut down the system.

⚠ Caution:

Before you unplug the AC power cord, always perform the following shutdown procedure. This procedure flushes any pending data to ensure data integrity.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Shut down the system:

   ```
   sys shutdown
   ```

3. Before you unplug the power cord, wait until you see the following message:

   ```
   System Halted, OK to turn off power
   ```

Example

Shut down a running system.

```
Switch:1#sys shutdown
Are you sure you want shutdown the system? Y/N  (y/n) ? y
CP1  [05/08/14 15:47:50.164] 0x00010813 00000000 GlobalRouter HW INFO System shutdown
initiated from CLI
CP1  [05/08/14 15:47:52.000] LifeCycle: INFO: Stopping all processes
CP1  [05/08/14 15:47:53.000] LifeCycle: INFO: All processes have stopped
CP1  [05/08/14 15:47:53.000] LifeCycle: INFO: All applications shutdown, starting power
down sequence
INIT: Sending processes the TERM signal
Stopping OpenBSD Secure Shell server: sshdno /usr/sbin/sshd found; none killed
Stopping vsp...Error, do this: mount -t proc none /proc
done
sed: /proc/mounts: No such file or directory
sed: /proc/mounts: No such file or directory
sed: /proc/mounts: No such file or directory
Deconfiguring network interfaces... done.
Stopping syslogd/klogd: no syslogd found; none killed
Sending all processes the TERM signal...
Sending all processes the KILL signal...
/etc/rc0.d/S25save-rtc.sh: line 5: /etc/timestamp: Read-only file system
Unmounting remote filesystems...
Stopping portmap daemon: portmap.
Deactivating swap...
Unmounting local filesystems...
[24481.722669] Power down.
[24481.751868] System Halted, OK to turn off power
```

Important information and restrictions

This section contains important information and restrictions you must consider before you use the switch.

Supported browsers

The switch supports the following browsers to access Enterprise Device Manager (EDM):

- Microsoft Internet Explorer 8.0
- Mozilla Firefox 32

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 the following documents:

- For the VSP 8000 series, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600.
- For the VSP 4000 series, see *Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600.

Enhanced secure mode versus hsecure mode

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/security/auditor	rwa/rw/ro/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	The same
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/Delete.	Standard op

Table continues…

Feature	Enhanced secure	Hsecure
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/Disable	Disabled
Telnet/FTP	Site Admin to Enable/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 and install a license file, see the following documents:.

- For information on the VSP 4000 series, see*Administration for Avaya Virtual Services Platform 4000 Series,* NN46251-600 .
- For information on the VSP 8000 series, see *Administering Avaya Virtual Services Platform 8000 Series*, NN47227-600 and *Getting Started with Avaya PLDS for Avaya Networking Products*, NN46199-300.

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

SFP+ ports

SFP+ ports support 1G and 10G transceivers only.

For a complete list of supported SFPs and QSFPs, see Hardware compatibility on page 46 .

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.

Interoperability notes for VSP 4000 connecting to an ERS 8800

- For customers running version 7.1.x: The minimum software release is 7.1.3.1, however the recommended ERS 8800 software release is 7.1.5.4 or later. On switches using 8612 XLRS or 8812XL modules for the links connecting to the VSP 4000 the minimum software version is 7.1.5.4. The “spbm version” on the ERS 8800 must be set to “802.1aq”.
- For customers running version 7.2.x: The minimum software release is 7.2.0.2, however the recommended ERS 8800 software release is 7.2.1.1 or later. On switches using 8612 XLRS or 8812XL modules for the links connecting to the VSP 4000 the minimum software version is 7.2.1.1.
- Diffserv is enabled in the VSP 4000 port settings, and is disabled in the ERS 8800 port settings, by default.

Notes on combination ports for VSP 4000

When the VSP 4000 is reset, the peer connections for all ports, including combination ports 47 and 48 on VSP 4450GTX-HT-PWR+, will transition down. During the reset, the fiber ports remain down, but only the copper ports 47 and 48 come up periodically throughout the reset. The copper ports 47 and 48 come up approximately 15 seconds into the reset, remain up for approximately 60 seconds, and then transition down until the boot sequence is complete and all ports come back up.

The following is an example of the status of the combination ports during reset.

```
CP1 [03/18/70 09:55:35.890] 0x0000c5e7 00300001.238 DYNAMIC SET GlobalRouter HW INFO Link
Down(1/47)
CP1 [03/18/70 09:55:35.903] 0x0000c5e7 00300001.239 DYNAMIC SET GlobalRouter HW INFO Link
Down(1/48)

CP1 [03/18/70 09:55:49.994] 0x0000c5ec 00300001.239 DYNAMIC CLEAR GlobalRouter HW INFO
Link Up(1/48)
CP1 [03/18/70 09:55:50.322] 0x0000c5ec 00300001.238 DYNAMIC CLEAR GlobalRouter HW INFO
Link Up(1/47)

CP1 [03/18/70 09:56:43.131] 0x0000c5e7 00300001.238 DYNAMIC SET GlobalRouter HW INFO Link
Down(1/47)
CP1 [03/18/70 09:56:43.248] 0x0000c5e7 00300001.239 DYNAMIC SET GlobalRouter HW INFO Link
Down(1/48)
```

Cabled connections for both copper and fiber ports

The following limitations apply when the combination ports have cabled connections for both the copper and fiber ports.

- Do not use the fiber port and do not insert an SFP into the optical module slot in the following situations:
  - a copper speed setting of either 10M or 100M is required
  - a copper duplex setting of half-duplex is required

Note:

These limitations are applicable only when auto-negotiation is disabled. To avoid this limitation, use auto-negotiation to determine the speed to 10/100/1000 and to determine the duplex.

- The 100M-FX SFP requires auto-negotiation to be disabled. Therefore, auto-negotiation will also be disabled for the copper port. Configure peer switch to disable auto-negotiation.

Chapter 4: Software Upgrade

Image upgrade fundamentals

This section details what you must know to upgrade the switch.

Upgrades

Install new software upgrades to add functionality to the switch. Major and minor upgrades are released depending on how many features the upgrade adds or modifies.

Upgrade time requirements

Image upgrades take less than 30 minutes to complete. The switch continues to operate during the image download process. A service interruption occurs during the installation and subsequent reset of the device. The system returns to an operational state after a successful installation of the new software and device reset.

Before you upgrade the software image

Before you upgrade the switch, ensure that you read the entire upgrading procedure.

You must keep a copy of the previous configuration file (*config.cfg*), in case you need to return to the previous version. The upgrade process automatically converts, but does not save, the existing configuration file to a format that is compatible with the new software release. The new configuration file may not be backward compatible.

Image naming conventions

The switch software use a standardized dot notation format.

Software images

Software images use the following format:

Product Name.Major Release.Minor Release.Maintenance Release.Maintenance Release Update.tgz

For example, the image file name **VSP4K.3.0.1.0.tgz** denotes a software image for the VSP 4000 product with a major release version of 3, a minor release version of 0, a maintenance release version of 1 and a maintenance release update version of 0. TGZ is the file extension. Similarly, the image file name **VSP4K.4.0.0.0.tgz** denotes a software image for the VSP 4000 product with a major release version of 4, a minor release version of 0, a maintenance release version of 0 and a maintenance release update version of 0.

Interfaces

You can apply upgrades to the switch using the Avaya Command Line Interface (ACLI).

For more information about ACLI, see one of the following documents, based on the platform you are upgrading:

- *User Interface Fundamentals for Avaya Virtual Services Platform 4000 Series,* NN46251-103
- *Using ACLI and EDM on Avaya Virtual Services Platform 8000 Series*, NN47227-103

File storage options

This section details what you must know about the internal boot and system flash memory and Universal Serial Bus (USB) mass-storage device, which you can use to store the files that start and operate the switch.

The switch file system uses long file names.

Internal flash

The switch has two internal flash memory devices: the boot flash memory and the system flash memory. The system flash memory size is 2 gigabytes (GB).

Boot flash memory is split into two banks that each contain a different copy of the boot image files. Only the Image Management feature can make changes to the boot flash.

The system flash memory stores configuration files, runtime images, the system log, and other files. You can access files on the internal flash through the /intflash/ folder.

File Transfer Protocol

You can use File Transfer Protocol (FTP) to load the software directly to the switch, or to download the software to the internal flash memory or USB device.

The switch can act as an FTP server. If you enable the FTP daemon (ftpd), you can use a standards-based FTP client to connect to the Control Processor (CP) module by using the ACLI log on parameters. Copy the files from the client to either the internal flash memory or USB device.

Saving the configuration

Save the configuration

- When you make a change to the configuration.
- To create a backup configuration file before you upgrade the software on the switch.

After you change the configuration, you must save the changes on the device. Save the configuration to a file to retain the configuration settings.

About this task

File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support IPv4 addresses.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Save the running configuration:

   ```
   save config [backup WORD<1-99>] [file WORD<1-99>] [verbose]
   ```

Example

```
Switch:1> enable
```

Save the configuration to the default location:

```
Switch:1# save config
```

Identify the file as a backup file and designate a location to save the file:

```
Switch:1# save config <filename>
```

Variable definitions

Use the data in the following table to use the **`save config`** command.

Variable	Value
backup *WORD<1–99>*	Saves the specified file name and identifies the file as a backup file. *WORD<1–99>* uses one of the following format: • a.b.c.d:<file> • /intflash/<file> • /usb/<file> The file name, including the directory structure, can include up to 99 characters.
file *WORD<1–99>*	Specifies the file name in one of the following format: • a.b.c.d:<file> • /intflash/<file> • /usb/<file> The file name, including the directory structure, can include up to 99 characters.
verbose	Saves the default and current configuration. If you omit this parameter, the command saves only parameters you change.

Upgrading the software

Perform this procedure to upgrade the software on the switch. This procedure shows how to upgrade the software using the internal flash memory as the file storage location.

To access the new software visit the Avaya support site: www.avaya.com/support. You need a valid user or site ID and password.

Use one of the following options to upload the file with the new software to the switch:

- Use FTP to transfer the file.
- Download the file to your computer. Copy the file to a USB device and insert the USB device into the USB port on the switch.

Note:

There is a limit of six software releases that can be stored on the switch. If you have six releases already stored on the switch, then you will be prompted to remove one release before you can proceed with adding and activating a new software release.

For information about removing a software release, see Deleting a software release on page 75.

Important:

See the tables below for a listing of the upgrade paths that are supported for each platform.

Table 11: Supported upgrade paths on the VSP 4850GTS and VSP 4850GTS-PWR+

Upgrade path	Support
Upgrade from 4.0 to 4.2	Supported
Upgrade from 4.1 to 4.2	Supported

Table 12: Supported upgrade paths on the VSP 4450GSX-PWR+

Upgrade path	Support
Upgrade from 4.0 to 4.2	Supported
Upgrade from 4.0.50 to 4.2	Supported
Upgrade from 4.1 to 4.2	Supported

Table 13: Supported upgrade paths on the VSP 4450GTX-HT-PWR+

Upgrade path	Support
Upgrade from 4.0 to 4.2	Supported
Upgrade from 4.0.40 to 4.2	Supported
Upgrade from 4.1 to 4.2	Supported

Table 14: Supported upgrade paths on the VSP 8284

Upgrade path	Support
Upgrade from 4.0 to 4.2	Supported
Upgrade from 4.0.1 to 4.2	Supported
Upgrade from 4.0.50 to 4.2	Supported
Upgrade from 4.1 to 4.2	Supported

Before you begin

- Back up the configuration files.
- Use an FTP application or USB device to upload the file with the new software release to the switch.
- Ensure that you have not configured VLAN 4060. If you have, you must port all configuration on this VLAN to another VLAN, before you begin the upgrade.

  Caution:

  Starting from Release 3.1, VLAN 4060 is not supported, and all configuration on this VLAN from previous releases will be lost after the upgrade.

Note:

Software upgrade configurations are case-sensitive.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. If you are using the USB port to transfer the files, go to the next step. If you are using FTP to download the files, enable FTP:

   ```
   boot config flag ftpd
   ```

3. Download the files to the switch through FTP or transfer them to the switch through the USB port.
4. Enter Privileged EXEC configuration mode by exiting the Global Configuration mode.

   ```
   exit
   ```

5. Extract the release distribution files to the /intflash/release/ directory:

   ```
   software add WORD<1-99>
   ```

6. Install the image:

   ```
   software activate WORD<1-99>
   ```

7. Restart the switch:

   ```
   reset
   ```

Important:

After you restart the system, you have the amount of time configured for the commit timer to verify the upgrade and commit the software to gold. If you do not commit the software to gold and auto-commit is not enabled, the system restarts with the last known working version after the commit timer has expired. This feature ensures you can regain control of the system if an upgrade fails.

8. After you restart the switch, enter Privileged EXEC configuration mode:

   rwa

   ```
   enable
   ```

9. Confirm the software is upgraded:

   ```
   show software
   ```

10. Commit the software:

    ```
    software commit
    ```

Example

The following example is for the VSP 4000, but the same steps apply to other switches.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#copy /usb/VSP4K.4.2.0.0.tgz /intflash/VSP4K.4.2.0.0.tgz
Switch:1>exit
Switch:1#software add VSP4K.4.2.0.0.tgz
Switch:1#software activate 4.2.0.0.GA
Switch:1#reset
Switch:1#show software
================================================================================
                    software releases in /intflash/release/
================================================================================
VSP4K.4.2.0.0int001 (Backup Release)
4.2.0.0.GA (Primary Release)

--------------------------------------------------------------------------------
Auto Commit     : enabled
Commit Timeout  : 10 minutes
Switch:1#software commit
```

Verifying the upgrade

Verify your upgrade to ensure proper switch operation.

Procedure

1. Check for alarms or unexpected errors:

   ```
   show logging file tail
   ```

2. Verify all modules and slots are online:

   ```
   show sys-info
   ```

Committing an upgrade

Perform the following procedure to commit an upgrade.

About this task

The commit function for software upgrades allows maximum time set by the commit timer (the default is 10 minutes) to ensure that the upgrade is successful. If you enable the auto-commit option, the system automatically commits to the new software version after the commit timer expires. If you disable the auto-commit option, you must issue the software commit command before the commit timer expires to commit the new software version, otherwise the system restarts automatically to the previous (committed) version.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. **(Optional)** Extend the time to commit the software:

   software reset-commit-time [<1–60>]

3. Commit the upgrade:

   ```
   software commit
   ```

Downgrading the software

Perform this procedure to downgrade the switch from the current trusted version to a previous release.

Important:

In release 4.2, the encryption modules are included in the image file. Therefore, the load-encryption menu is present but no longer applicable to the current release. You do not require an ACLI command to load it.

After you downgrade from release 4.2 to a previous release, and you try to execute the command **soft add-modules**, you may get the following error message: “Command not allowed in this release. The Encryption modules are loaded along with the application image”.

Workaround: Boot the downgraded release first; then load the encryption modules as follows:

1. Downgrade to older version.
2. Add the encryption modules: **soft add-modules <soft version><module file>**.
3. Load the encryption modules: **load-encryption <AES|DES|3DES>**.

Before you begin

Ensure that you have a previous version installed.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Activate a prior version of the software:

   ```
   software activate WORD<1-99>
   ```

3. Restart the switch:

   ```
   reset
   ```

   Important:

   After you restart the system, you have the amount of time configured for the commit timer to verify the software change and commit the software to gold. If you do not commit the software to gold and auto-commit is not enabled, the system restarts with the last known working version after the commit timer expires. This feature ensures you can regain control of the system if an upgrade fails.

4. Commit the software change:

   ```
   software commit
   ```

   Important:

   If you do not enable the auto-commit functionality, you must commit the software change before the commit timer expires. This is an optional step otherwise.

5. Verify the downgrade:
   - Check for alarms or unexpected errors using the `show logging file tail` command.
   - Verify all modules and slots are online using the `show sys-info` command.
6. (Optional) Remove unused software:

   ```
   software remove WORD<1-99>
   ```

Variable definitions

Use the data in the following table to use the `software` command.

Variable	Value
activate WORD<1-99>	Specifies the name of the software release image.
add WORD<1-99>	Specifies the path and version of the compressed software release archive file.
remove WORD<1-99>	Specifies the path and version of the compressed software release archive file.

Deleting a software release

Perform this procedure to remove a software release from the switch.

Note:

There is a limit of six software releases that can be stored on the switch. If you have six releases already stored on the switch, then you will be prompted to remove one release before you can proceed with adding and activating a new software release.

Procedure

1. Enter Privileged EXEC configuration mode:

   ```
   enable
   ```

2. Remove software:

   ```
   software remove WORD<1-99>
   ```

Example

The following example is for the VSP 4000 switch, but the same steps can be used for other switches.

```
VSP-4450GSX-PWR+:1>enable
VSP-4450GSX-PWR+:1#software remove VSP4K.4.1.0.0.tgz
```

Chapter 5: Known issues and limitations

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

Related Links

Known issues in this release for Avaya VSP 4000, VSP 8200, and VSP 8400 on page 76

Known issues in this release for Avaya VSP 4000, VSP 8200, and VSP 8400

This section identifies the known issues in this release for the Avaya VSP 4000, VSP 8200, and VSP 8400.

Device related issues

Table 15: 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`.
wi01166763	SLAMon tests fail (between 2% and 8% failure) between VSP 4000 devices when you have too many agents involved with scaled configurations.	This happens only in a scaled scenario with more than seven agents, otherwise the failure does not occur. The acceptable failure percentage is 5%, but you may see failures of up to 8%.
wi01168610	**VSP 4450GSX**: The command **`sys shutdown`** does not change the STATUS LED on the VSP 4450GSX-PWR+ device.	None. This issue does not impact any functionality.
wi01168706	The following error message occurs when performing **`shutdown/no-shutdown`** commands continuously: `IO1 [05/02/14 06:59:55.178:UTC] 0x0011c525 00000000 GlobalRouter COP-SW ERROR vsp4kTxEnable Error`	None. When this issue occurs, the port in question may go down, then performs a **`shutdown/no-shutdown`** of the port to bring it up and resumes operation.

Table continues…

Issue number	Description	Workaround
	`changing TX disable for SFP module: 24, code: -8`	
wi01171802	**VSP 4450GSX**: On a fresh boot, peer ports connected to ports 1/49 and 1/50 bounce and may cause additional transitions in the network.	None.
wi01171907	**VSP 4450GSX**: CAKs are not cleared after setting VSP 4K to factory-default.	None. Currently this is the default behavior and does not affect functionality of the MACsec feature.
wi01173026	A reboot with verbose configuration does not allow you to delete any vrf.	This issue occurs only when the configuration file is saved in “verbose” mode and then rebooted in that configuration. On field, it is highly unlikely to save a configuration file in verbose mode and use that for sourcing the configuration. Verbose mode is used more as a diagnostic tool. This issue does not impact the functionality of the product.
wi01173136	**T1 SFP**: Shutting down the T1 link from one end of the VSP 4000 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 T1 SFP link from one end is shutdown. Enable a dynamic link layer protocol such as LACP or VLAC on both ends to shut the remote end down too. As an alternative, administratively disable both the 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 of packets so that the application might receive a slow response. But in this case, it is a marginal increase in the packet count, that occurs due to PN mismatch sometimes only during Key expiry, and does not induce any latency.	None.
wi01195988	IPv4 Ping/TraceRoute may not work in the EDM.	Use ACLI to initiate ping and traceroute.
wi01196000	Not able to ping or do traceroute to IPV4 address using EDM.	Use ACLI to initiate ping and traceroute.
wi01208650	The Console gets disconnected frequently when “screen trace” is enabled (trace screen enable). The error displayed is “Forced log-out after 65535 secs”.	None.

Table continues…

Issue number	Description	Workaround
wi01212099	COM EDM Plugin L2 Traceroute IPv6 does not work properly and gives the error, “No Such Name".	Use the ACLI to initiate the L2 Traceroute IPv6.
wi01210286	The IPv4 and IPv6 icmp redirect functionality does not work as expected. This pertains to the “ip icmp redirect” and the “ipv6 icmp redirect-msg” CLI commands. If an IPv4 or IPv6 packet is L3-routed back out through the same interface on which a packet came in, two things should happen: 1. The original packet should be sent back out on the same interface on which it came in. 2. If the ipv4/ipv6 redirect flag is set, an ICMP redirect message should be sent back to the source. Step 1 still occurs, but step 2 does not. In other words, the redirect message is not sent.	None.
wi01174787	Using EDM, you cannot create static ARP entries.	Use the ACLI **`config ip arp`** command to create static ARP entries.
wi01203006	After creating an IPv4 filter to redirect next hop, the traffic does not get redirected to the new route even though the filter is hit and the next hop IP is reachable.	This issue occurs when the net hop IP is not reachable on rebooting the switch. Reconfigure the redirect next hop filter for ACLs once the route is up after reboot.
wi01204999	VSP devices as intermediate nodes, do not respond to the link trace request.	VSP devices fail to respond to CFM link trace requests if the SPBm BVLANs are deleted and recreated with different BVLAN IDs. Issuing a node reboot after BVLAN ID change will restore Linktrace operation.
wi01207076	If both IPv4 and IPv6 are configured on a vlan interface. Whenever IPv6 MTU is changed, IPv4 MTU also gets changes for that interface.	Set a higher MTU value upto 9500 bytes instead of the default MTU size of 1500 bytes that gets set when IPv6 is enabled on the vlan.
wi01207546	In configurations with at least three VRRP nodes with Back Master enabled on a non-SPB VLAN the VRRP state may continuously fluctuate between Master and Backup Master. Forwarding is not affected.	Only enable VRRP Backup Master if the node is running SPB and the VLAN is an SPB C-VLAN, for instance, an SMLT VLAN on a vIST node, otherwise do not enable VRRP Backup Master.
wi01208362	VSPtalk is referenced in "show fulltech". This has no impact on the switch operation.	None.

Table continues…

Issue number	Description	Workaround
wi01209346	In 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	Use a v3 interface as querier in a LAN segment which has snoop enabled v2 and v3 interfaces.
wi01209532	The port led on the device remains steady amber after removing the SFP+ pluggable from the port. This has no impact on the switch operation.	None.
wi01210104	In EDM, you cannot select multiple 40–gigabit ports or a range of ports that includes 40–gigabit ports to graph or edit them. You need to select them and edit them individually.	None.
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.	Insert the QSFP+ carefully. If the port gets damaged, it needs to be repaired.
wi01201333	In EDM, when bgp confederation identifier or bgp confederation peers are configured, 4-byte-as numbers are not supported.	Use the ACLI command for this parameter.
wi01209604	From EDM, you cannot perform an L2 IP-PING for an Ipv6 address. EDM gives the error, “No next Hop address found for ip address provided”.	Use the ACLI perform an L2 IP-PING.
wi01212115	On EDM, the port LED for channelized ports only shows the status of sub-port #1, but not to the rest 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.
wi01207396	"In-Discard" counter gets increments continuously between V-IST peer interface while you enable vlacp on T-UNI MLT.	None.
wi01215216	In enhanced secure mode, If your user level is Security or Auditor, the **`show logging`**	None.

Table continues…

Issue number	Description	Workaround
	command is displayed but is not functional. The “Show Logging” Command should not be displayed. logging parameters still appear in the help text for the **`show logging`** command, but you cannot access this command if you have the Security or Auditor access level.	
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 configuration on device, and reboot again.
wi01214025	Traffic is getting forwarded to igmp v2 SSM group, even after deleting igmp ssm-map entry for the group.	If the delete action is performed first, it is fine to re-create the ssm-map record; then disable the ssm-map record. The disabled ssm-map record will then cause the receiver to timeout, as any subsequent membership reports that arrive which match the disabled ssm-map record will then be dropped, thus allowing for the receiver to timeout. The ssm-map record can then be deleted after the receivers time out.
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 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 you may need to meet. The actual minimum password requirements you need to meet are configured on your system by the administrator.	None.
wi01212591	IPv4 shortcut traffic is going to queue 0 on non-gateway device of the vist pair. The packet may be en-queued incorrectly, so if the queue is congested, the packet maybe unexpectedly dropped. Or if such kind of packet causes queue congestion, then the incorrect queue would be congested.	None.

Table continues…

Issue number	Description	Workaround
	Note that this wi is specific to the VSP 4000.	
wi01204456	On rare occasions, after a chassis reboot, it is possible for one or two ports on ESMs in slots 1 and 2 to fail. These port failures do not occur on an operational system. Ports on ESMs in slots 3 and 4 are not affected. The characteristics of a port failure are as follows: For ESMs 8424XS, 8418XSQ and 8418XSQ: • 40Gig and 10Gig ports: The port will not link up (includes QSPF+, SPF+ and DAC). • 1Gig ports: The port may link up but will not receive traffic. For ESM 8424XT: • 10Gig/1Gig/100M ports: The port will not link up. Depending on the card type the ports that may fail are the following: • 8424XS and 8418XSQ: Port 9 and/or 17 • 8424XT: Port 10 and/or 18 • 8408QQ: Port 3 and/or 5	A chassis reboot is required to recover the failed ports. A failure-detection mechanism has been implemented to detect this fault and raise an alarm during system initialization. The administrator can then chose to reset the chassis if the failed port(s) are required for operation.
wi01216535	The “router ospf” entry always appears in the configuration file regardless of whether OSPF is configured or not. This line does not perform any configuration and has no impact on the running software.	None.
wi01216550	When you use telnet/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.
wi01215773	The switch provides an NTP log message indicating that the NTP server did not sync up, even though one of the NTP servers synchronized correctly and the NTP stats show that it did.	None.
wi01216496	The output of the "show cli password" command provides the password rules for non-Admin users. This output should provide the rules for Admin users. As an admin user, you must have "min-passw-len 15" and "password-rule 2 2 2 2".	None.

Related Links

Known issues and limitations on page 76
Limitations in this release in VSP 4000 on page 82

Limitations in this release in VSP 4000

This section lists known limitations and expected behaviors that may first appear to be issues. The following table provides a description of the limitation or behavior and the work around, if one exists.

Caution:

The alpha release of the VSP 4450GTX-HT-PWR+ has operating temperature and power limitations. For safety and optimal operation of the device, ensure that the prescribed thresholds are strictly adhered to.

Table 16: VSP 4450GTX-HT-PWR+ limitations

Issue	Description	Workaround
For high-temperature threshold	The VSP 4450GTX-HT-PWR + supports a temperature range of 0°C to 70°C. In the alpha release, power supply does not shut down at an intended over-temperature threshold of 79°C.	To prevent equipment damage, ensure that the operating temperature is within the supported temperature range of 0°C to 70°C.
For power supply wattage threshold	Software functionality to reduce the POE power budget based on the number of operational power supplies and operating temperature is not available in the Alpha SW image.	Ensure that the POE device power draw is maintained at the following when the device is at temperatures between 61°C and 70°C: • 400W — with 1 operational power supply • 832W — with 2 operational power supplies
For inoperable external USB receptacle	The VSP 4450GTX-HT-PWR+ has an empty external USB receptacle that was not available in GTS models. Software to support the use of the external USB receptacle is not yet available in the Alpha SW image. Therefore the USB port is inoperable.	No workarounds are provided with the alpha image.

Table 17: Limitations and expected behaviors

Issue number	Description
wi01159075	**VSP 4450GSX-PWR+**: Mirroring functionality is not working for RSTP BPDUs
wi01145099	IP multicast packets with TTL=1 are not switched across the SPB cloud over an L2 VSN. They are dropped by the ingress BEB. To prevent IP multicast packets from being dropped, configure multicast senders to send traffic with TTL >1.
wi01138851	Configuring and Retrieving licenses using the EDM is not supported.
wi01112491	IS-IS enabled ports cannot be added to an MLT. The current release does not support this configuration.
wi01142142	When a multicast sender moves from one port to another within the same BEB, 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 L3 interface, you can toggle the IGMP state. **Caution:** Expect traffic loss until IGMP records are built after toggling the IGMP state.
wi01143223	Hosts connected to a VSP 4000 system acting as a VRRP backup-master, cannot ping the VRRP virtual IP, if the VRRP session is established over an L2–VSN between the VRRP master and backup-master for that VLAN. However, traffic from the hosts is routed by the VRRP backup-master, and the ARP for the VRRP virtual IP is resolved.
wi01141638	When a VLAN with 1000 multicast senders is deleted, the console or telnet session hangs and SNMP requests time out for up to 2 minutes.
wi01137195	A static multicast group cannot be configured on an L2 VLAN before enabling IGMP snooping on it. After IGMP snooping is enabled on the L2 VLAN for the first time, static multicast group configuration is allowed, even when IGMP snooping is disabled later on that L2 VLAN.
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`.
wi01122478	Stale snmp-server community entries for different VRFs appear after reboot with no VRFs . On an node with any valid config file saved with more than the default vrf0 , snmp_community entries for that VRF are created and maintained in a separate txt file, snmp_comm.txt, on every boot. The node reads this file and updates the snmp

Table continues…

Issue number	Description
	communities available on the node. As a result for a boot with config having no VRFs, you may still see snmp_community entries for VRFs other than the globalRouter vrf0 .
wi01171670	Telnet packets get encrypted on MACsec enabled ports.
wi01198872	Loss of learned MAC addresses occurs in a vIST setup beyond 10k addresses. In a SPB setup the MAC learning is limited to 13k MAC addresses, due to the limitation of the internal architecture when using SPB. Moreover, as vIST uses SPB and due to the way vIST syncs MAC adresses with a vIST pair, the MAC learning in a vIST setup is limited to 10K Mac addresses.

Related Links

Known issues in this release for Avaya VSP 4000, VSP 8200, and VSP 8400 on page 76

Chapter 6: Resolved issues

Resolved issues for Avaya VSP 4000, VSP 8200, and VSP 8400

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

Fixes from previous releases: Release 4.2 incorporates all fixes from prior releases, up to and including Release 4.1.

Table 18: Resolved issues in this release

WI reference	Description	Workaround
wi01162515	The VSP 4000 switch fails to enable maximum supported ingress (1536) and egress (256) ACEs.	None.
wi01111785	Internal QoS remapping with filters does not work for certain UDP destination ports. This is due to the control packets in the VSP 4000 system that are assigned with a higher priority egress queue. The action to assign the incoming control packet with an egress queue is in conflict with the action of the egress queue derived from the internal QoS remapping with ACL filter. Hence, the internal QoS remapping with ACL filter does not work for those control packets.	The control packets received from the ingress port include the following: • Always assign queue-6: DHCP, BPDU, LLDP, SLPP, CFM, ARP, IST-ARP1, IST-SLM, BARP, EAP, PIM-MC, PIM-UC, RIPv2, RIPv1, OSPF-MC, OSPF-UC, IGMP, BGP, TELNET, SSH, RSH, RLOGIN, TFTP, FTP, RADIUS, NTP, ICMP, HTTP, HTTPS, IPV6-ND. • Always assign queue-7: ISIS control, LACP, VLACP, VRRP, SNMP, IST
wi01126761	Traffic convergence can take 3 to 6 seconds for NNI failover on a BEB with a large number (greater than 600) of L2 VSNs.	None
wi01134468	On a T-UNI port with L2 untrusted configuration, the internal QoS of the traffic flow is derived from the .1p bits of the ingress tagged traffic. If incoming client packets are tagged, the VSP 4000 system always derives the internal priority queue from the 802.1p tag.	None.

Table continues…

WI reference	Description	Workaround
wi01134509	On a T-UNI port, with incoming untagged traffic, the internal QoS level of the traffic flow is set to 0, irrespective of the L2 Trust configuration on the port. If incoming client packets are untagged, the internal priority queue of the VSP 4000 is always the best-effort queue.	None.
wi01134624	With an 8 port NNI MLT, a VSP 4000 system acting as BEB can support up to 600 multicast streams.	None
wi01135628	Remarking of dot1p for tagged unicast, unknown unicast or multicast traffic fails on L2 trusted T-UNI ports. This issue is not seen on CVLAN ports.	For any incoming packet on a T-UNI port, you can remark traffic using internal-qos to set the QoS level instead of remark-dot1p.
wi01136168	The `metric` field in the `redistribute` command is not supported for inter-VRF redistributed routes. This impacts only inter-VRF metric settings. It does not impact inter-VRF route filtering.	None
wi01136327	**T-UNI, QoS**: The .1p bit in the CVLAN of the egress packet is changed when ingress .1p is 0, and also when ingress .1p is 1 in the case of L2 Trusted with L3 Untrusted and Diffserv disabled.	None. There is no impact to packet processing. The issue is seen only if you mirror the packet in the SPB cloud.
wi01136379	A node configured with all supported features and booted with the base license loses all T-UNI configuration. Loading a node with a base license fails to load configuration related to the IP VRF, ISIS, SPBM and IPVPN.	None
wi01137696	A port or a VLAN based filter created for CFM, OSPF, RIP, PIM, or VRRP control protocols with a Deny/Permit action (ACE or Global-ctrl-pkt action), based on ethertype/ip/other qualifiers, bypasses the filter rules. A port based filter created on T-UNI port or MLT for LACP, VLACP control protocols with a Deny/Permit action (ACE or Global-ctrl-pkt action), based on ethertype/ip/other qualifiers, bypasses the filter rules.	None
wi01137736	On a base VSP 4000 system with Revision 10 hardware and POE support, PAUSE frames are not supported.	None
wi01138070	The 802.1 priority bits in the BVLAN tag are not copied to the I-Tag when traffic egresses out of the NNI port.	None

Table continues…

WI reference	Description	Workaround
wi01140395	Pinging a remote IP address over VRF does not work unless the source IP address is specified.	None. This behavior is as designed.
wi01141161	Traffic is not forwarded on a T-UNI LACP MLT, if the LACP MLT is *not* associated with a VLAN before adding to a T-UNI ISID.	Ensure that the LACP MLT is associated with a VLAN before adding to a T-UNI ISID. The associated VLAN can also be the default VLAN.
wi01141429	The error message `GlobalRouter POE ERROR poeMgrPoeDefaultConfig: POE Driver error (bcm_poe_set_logical_port_map()` can be ignored if seen once or twice during boot up.	If the error message persists, verify that the POE driver on the hardware is up and running.
wi01142915	When you execute the **`default SLPP`** command without parameters, the command does not automatically set all SLPP parameters to default.	Always execute the `default SLPP` command with appropriate parameters. For example, to set the SLPP parameter `tx-interval` to default, execute the command `default slpp tx-interval`.
wi01143509	Redundant RIP configuration is saved for BVLANs when configuration is saved in verbose mode. Sourcing this configuration displays the error `RIP circuit for ifindex does not exist`.	None
wi01154179	**VSP 4450GSX-PWR+**: No log messages are generated when plugging/unplugging the USB from the switch.	None.
wi01157224	Killing the “TOP” process from the Shell may crash the system. This issue has occurred only once and was not reproducible.	None.
wi01159644	The output of the command **`show spanning-tree rstp port config [{slot/port[-slot/port][,...]}]`** displays the value of Port Protocol Migration as `false` irrespective of whether the protocol migration flag is set to `true` or `false`.	None. This behavior is as designed.
wi01160332	**VSP 4450GSX-PWR+**: The command **`show int gi statistic verbose`** shows half the packet count on MACsec port ingress.	This happens only with the MACsec IXIA port. This issue does not appear on a real back-back connected scenario.
wi01161534	**VSP 4450GSX-PWR+** (PoE): The 802.3af standard allows 21W of power to PD.	Run the **`poe poe-limit <>`** to limit the power to 15.4W if 802.3af standard is configured.
wi01175367	The voltage for power supply erroneously displays as 220 volts when the power intake is more than	None.

Table continues…

WI reference	Description	Workaround
	1000 W, regardless of the actual power supply voltage (110 or 220 volts). You should read this as 110/220 volts. For AC power, the power voltage displays as 110/220 volts for all other cases.	
wi01198259	ISIS routes stop being redistributed by a DUT after executing a particular set of ISIS Accept policy test cases.	Apply the accept policies again.
wi01197547	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 BMAC, 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.	None.
wi01203053	When there are two equal cost routes to a destination in different areas, increasing the cost of the learned interface more than the other interface has no effect on the route.	The issue is seen only when increasing the cost and only for inter-area routes. The issue is not seen when decreasing the cost. To see the effect on the route, disable and then enable OSPF after increasing the cost.
wi01204121	On using the command `show interface gigabitethernet statistics`, the OUTLOSS PACKETS counter value increments when packets are dropped as a result of Source Port squelching on NNI ports.	None.
wi01205505	IPv6 ERCD and RCIP6 error logs are observed following IST reset. You may see the following errors when all RSMLT enabled VIST and UNI ports are shutdown: • REPLACE neighbor to HW FAILED • DELETE neighbor from HW FAILED • Failed to lookup Nexthop • Failed to update the stale bit for Neighbor The errors are logged intermittently when all NNI/ VIST and UNI ports with RSMLT are shutdown or reset. These error logs occur due to the existence of a timing window during which RSMLT may try to clean-up VLAN when the port is already down.	Ignore these errors as there are no other ramifications and they do not cause any data loss.

Table continues…

WI reference	Description	Workaround
wi01205572	Spoof-detect may not work when enabled. There are no commands to check the status of a spoof-detect port.	None.
wi01205594	When CIST is disabled by admin, deleting an ISIS interface at port level may automatically enable CIST level mstp state.	None.
wi01207711	SPB ethertype 0x8100 is modfied to 0x88a8 when packets traverse over Virtual IST.	None.
wi01209696	A corner case scenario where an IGMP ACL is applied to block a host from joining a particular group, while the Join record already exists for that host on the VSP, and if that host happens to be the only receiver on that interface, results in a node reboot. This happens only on IGMPv3 snoop enabled interface.	Use ACLs, even if you want to block the only receiver available on the interface.
wi01206933	Users may experience unresponsive ACLI sessions after using the **`trace screen enable`** command.	None.
wi01211152	The switch selects the route that it receives from the route-reflector in the routing table rather than the one that it receives over confederation eBGP.	None.
wi01212817	The switch does not report remote faults properly. It takes down the port, but it reports the faults as a local faults, even when they are remote faults.	None.
wi01209895	When IST signals a MAC update, the local UNI port traffic experiences and instance of temporary flooding.	None.
wi01211190	Users may observe the TX-NNI port in console messages during a reboot. These messages are typically seen in a highly scaled environment where the switch must process control or data packets for an extended period of time. Such messages can be ignored. Messages with the TX-NNI port encountered in other scenarios should be investigated in an appropriate manner.	None.
wi01204999	VSP devices as intermediate nodes, do not respond to the link trace request.	VSP devices fail to respond to CFM link trace requests if the SPBm BVLANs are deleted and recreated with different BVLAN IDs. Issuing a node reboot after BVLAN ID change will restore Linktrace operation.
wi01208787	The configuration does not load properly when you reboot the switch after pulling out a 40–gigabit card with channelized ports in an mlt group. When you	None.

Table continues…

WI reference	Description	Workaround
	pull out the 40–gigabit card and reboot the switch, all the ports in the mlt group or groups are missing.	
wi01207396	"In-Discard" counter gets increments continuously between V-IST peer interface while you enable vlacp on T-UNI MLT.	None.
wi01215834	VSPTalk commands are visible in this release, but this feature is not supported.	None.
wi01200896	On a VSP4000 switch under `show qos cosq-stats cpu-port` command drop packets counter gets incremental on CPU COS 1. In customer network , NETBIOS packets around (250 -350 PPS) resulted in packet drop in the broadcast queue as the queue size was small.	None.