



Avaya Virtual Services Platform 4000 Release Notes - Release 4.1

Release 4.1
NN46251-401
Issue 07.03
April 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](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	6
Purpose.....	6
Related resources.....	6
Support.....	9
Chapter 2: New in Release 4.1	11
Features.....	11
Overview of features and hardware models by release.....	15
VSP 4000 and VSP 8000 feature differences.....	23
Other Changes	24
Chapter 3: Important notices	25
Hardware compatibility.....	25
Platform power supplies.....	27
Software scaling capabilities.....	28
File names for release 4.1.....	31
Calculating and verifying the md5 checksum for a file on a switch.....	33
Calculating and verifying the md5 checksum for a file on a client workstation.....	34
Important information and restrictions.....	35
Interoperability notes for VSP 4000 connecting to an ERS 8800.....	35
Supported browsers.....	35
User configurable SSL certificates.....	35
Feature licensing.....	36
Combination ports.....	38
SFP and SFP+ ports and use of lower speed transceivers.....	38
Shutting down VSP 4000.....	39
Interoperability notes for VSP 4000 or VSP 8000 connecting with ERS 5650.....	40
Chapter 4: Software Upgrade	41
Image upgrade fundamentals.....	41
Image naming conventions.....	41
Interfaces.....	42
File storage options.....	42
Upgrading the software.....	42
Verifying the upgrade.....	45
Committing an upgrade.....	45
Downgrading the software.....	46
Deleting a software release.....	47
Chapter 5: Supported standards, RFCs, and MIBs	48
Supported IEEE standards.....	48
Supported RFCs.....	49
Standard MIBs.....	52

Proprietary MIBs.....	54
Chapter 6: Known issues and limitations.....	56
Known issues in release 4.1.....	56
Limitations in release 4.1.....	63
Chapter 7: Resolved issues in release 4.1.....	65

Chapter 1: Introduction

Purpose

This document describes important information about this release of the Virtual Services Platform 4000 (VSP 4000). 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 the *Avaya Virtual Services Platform 4000 Documentation Roadmap*, NN46251–100 for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, access the website 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

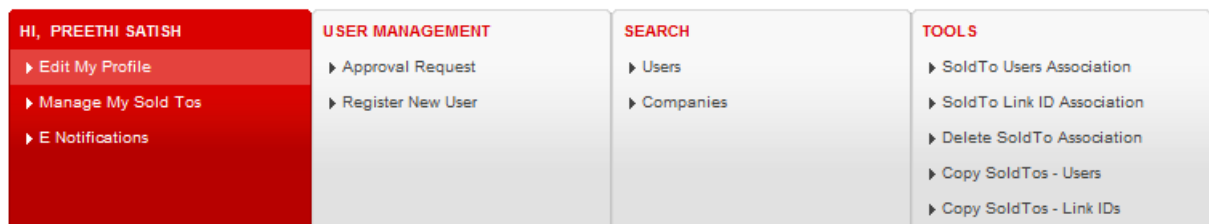
You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Ethernet Routing Switch 8800.

Procedure

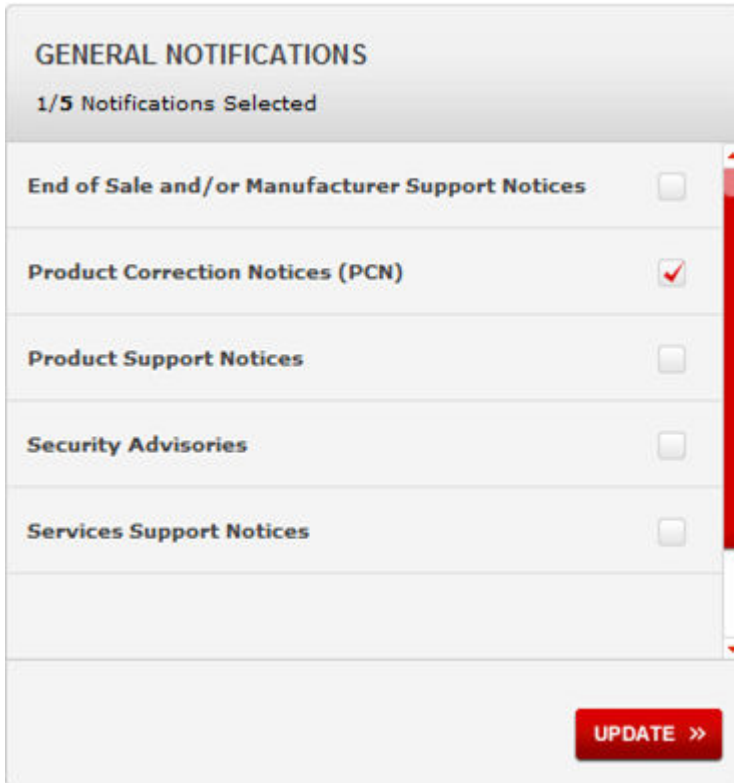
1. In an Internet browser, go to <https://support.avaya.com>.
2. Type your username and password, and then click **Login**.
3. Click **MY PROFILE**.



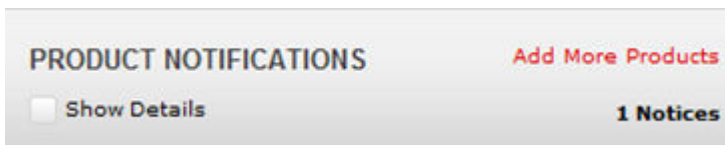
4. On the site toolbar, click your name, and then click **E Notifications**.



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.

The screenshot shows two side-by-side panels. The left panel, titled 'PRODUCTS', has a 'My Notifications' link in the top right. It contains a list of products: Virtual Services Platform 7000, Virtualization Provisioning Service, Visual Messenger™ for OCTEL® 250/350, Visual Vectors, Visualization Performance and Fault Manager, Voice Portal, Voice over IP Monitoring, W310 Wireless LAN Gateway, WLAN 2200 Series, and WLAN Handset 2200 Series. The right panel, titled 'VIRTUAL SERVICES PLATFORM 7000', has a 'Select a Release Version' dropdown menu set to 'All and Future'. Below this are several checkboxes: 'Administration and System Programming' (unchecked), 'Application Developer Information' (unchecked), 'Application Notes' (unchecked), 'Application and Technical Notes' (checked), 'Declarations of Conformity' (unchecked), and 'Documentation Library' (checked). A red 'SUBMIT >>' button is at the bottom right of the right panel.

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 Release 4.1

The following sections detail what is new in *Release Notes for Avaya Virtual Services Platform 4000 Series*, NN46251-401 for Release 4.1.

Features

See the following sections for information about feature-related changes.

IPv6

Release 4.1 introduces support for IPv6 routing.

Base IPv6 features:

- Dual-Stack IPv4/IPv6 support
- 6in4 Configured Tunnels to enable transition from IPv4 to IPv6 networks
- IPv6 Routing (Static, OSPFv3)
- Resilient IPv6 network design enabled by VRRPv3 and IPv6 support on SMLT/RSMLT links
- IPv6 connectivity for management protocols to enable RADIUSv6, DHCPv6, DNSv6 and Syslog servers in IPv6 network
- IPv6 OAM support including Ping, Traceroute, Telnet, FTP, TFTP, Rlogin, SSH, SNMPv3, EDM access via IPv6 HTTPS
- IPv6 Access Control Lists (ACLs)

Note:

The software does not support IPv4-mapped IPv6 addresses, for example, 0::FFFF:a.b.c.d, or IPv4-compatible IPv6 addresses, for example, 0::a.b.c.d.

IPv6 over Fabric:

- IPv6 shortcuts
- IPv6 routing between Layer 2 VSNs

For more information, see *Configuring IPv6 Routing on Avaya Virtual Services Platform 4000 Series*, NN46251-511.

IPv6 Access Control Lists (ACLs)

Release 4.1 adds support for IPv6 ingress port/vlan security ACL/Filters. VSP 4000 supports a maximum of 256 IPv6 ingress port/vlan security ACL/Filters. IPv6 ingress QoS ACL/Filters and IPv6

egress security and QoS ACL/Filters are not supported. For more information, see *Avaya Virtual Services Platform 4000 Series Configuration – QoS and ACL Based Traffic Filtering*, NN46251-502.

IPv6 shortcuts

Release 4.1 adds support for IPv6 Shortcuts, which function in a very similar manner to IPv4 Shortcuts. Both types of Shortcuts use IS-IS as the Interior Gateway Protocol (IGP) and the link-state packet (LSP) for reachability information. However, IPv4 Shortcuts use TLV 135 and IPv6 Shortcuts use TLV 236. All TLVs announced in the IS-IS LSPs are grafted onto the shortest path tree (SPT) as leaf nodes.

IPv6 Shortcuts use some IPv4 Shortcuts functionality so IPv4 Shortcuts must be enabled before you enable IPv6 Shortcuts. For more information, see *Configuration Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series*, NN46251–510.

IPv6 routing between Layer 2 VSNs

IPv6 routing between Layer 2 VSN (inter-VSN routing) allows configuration of any SPB IPv6 capable node to also provide Inter-ISID Layer 2 VSN routing by adding an IPv6 interface to a port-less CVLAN. IPv6 Unicast traffic can then be routed anywhere in the SPB fabric on SPB-IPv6 capable nodes. For more information, see *Configuring IPv6 Routing on Avaya Virtual Services Platform 4000 Series*, NN46251-511 and *Configuration Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series*, NN46251–510.

Intermediate System to Intermediate System (IS-IS) accept policies

Release 4.1 adds Intermediate System to Intermediate System (IS-IS) accept policies. You can use IS-IS accept policies with Layer 3 VSNs or IP Shortcuts to filter incoming IS-IS routes over the SPBM cloud. IS-IS accept policies enable the device to determine whether to add an incoming route to the routing table. IS-IS policies can also use either a service instance identifier (I-SID) or an I-SID list to filter incoming traffic.

For more information about IS-IS accept policies, see *Configuration Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series*, NN46251–510.

SMLT and RSMLT with vIST

Split MultiLink Trunking (SMLT) provides subsecond failover when a switch fails. Routed Split MultiLink Trunking (RSMLT) permits rapid failover for core topologies by providing an active-active router concept to core SMLT networks.

Virtual Inter-Switch Trunk (vIST) improves on this resiliency by using a virtualized IST channel through the SPBM cloud. For more information, see *Configuring Link Aggregation and MLT on Avaya Virtual Services Platform 4000 Series*, NN46251-503.

Simplified virtual Inter-switch Trunk (vIST)

Avaya introduced Simplified virtual Inter-switch Trunk (vIST) for non-SPB customers who are used to using SMLT with IST. The Simplified vIST feature provides a seamless migration of IST-based SMLT configurations to vIST-based SMLT configurations.

- Simplified vIST is available ONLY for non-SPB deployments when the boot flag (`spbm-config-mode`) is disabled.
- When the boot flag is enabled (default setting), Simplified vIST is not available so you can configure SPB/ISIS for vIST as described in the Link Aggregation document.

*** Note:**

Virtual IST is not supported on LACP-enabled MLTs.

For more information, see *Configuring Link Aggregation and MLT on Avaya Virtual Services Platform 4000 Series*, NN46251-503.

EAPoL IEEE 802.1x-2001 (Single Host Single Authentication)

Release 4.1 supports IEEE 802.1x based Extensible Authentication Protocol over LAN (EAPoL).

Extensible Authentication Protocol over LAN (EAPoL) is a port-based network access control protocol. EAPoL provides security by preventing users from accessing network resources before they are authenticated. The EAPoL authentication feature prevents users from accessing a network to assume a valid identity and access confidential material or launch denial-of-service attacks. For more information, see *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601.

PIM-SM

PIM-SM, as defined in RFC2362, supports multicast groups spread out across large areas of a company or the Internet. PIM-SM sends multicast traffic only to routers that specifically join a multicast group. For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series*, NN46251-504

PIM-SSM

Source Specific Multicast optimizes PIM-SM by simplifying the many-to-many model. Because most multicast applications distribute content to a group in one direction, SSM uses a one-to-many model that uses only a subset of the PIM-SM features. This model is more efficient and reduces the load on multicast routing devices. *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series*, NN46251-504

VMS Endura script

The `run vms endura` script is an ACLI command that is used to pre-configure basic and common configuration parameters to quickly and easily deploy an Endura Video Surveillance network in accordance with best practices using Avaya networking equipment.

With this script, you can perform the following:

- deploy Shortest Path Bridging
- enable full multicast capabilities between all IP subnets and VLANs using existing ACLI commands

For more information, see *Configuration Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series*, NN46251-510.

SPBM install script

Release 4.1 supports an ACLI script to quickly enable Avaya VENA Fabric Connect on a switch. You can use the command `run spbm` to quickly set up the SPB and IS-IS configuration.

The `run spbm` command enables you to modify the default parameters. The console displays each parameter with the default value in brackets, which you can modify by entering another value.

For more information, see *Configuration Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series*, NN46251-510.

VLACP statistics

Release 4.1 adds the ability to enable sequence numbers for VLACP PDUs to assist with monitoring dropped packets. New commands also enable you to display and clear VLACP statistics. For more information, see *Performance Management of Avaya Virtual Services Platform 4000 Series*, NN46251-701.

Licensing support

Starting with Release 4.1, Avaya Networking is moving to Product Licensing & Delivery System (PLDS) as the license order, delivery and management tool. PLDS provides self-service license activations, upgrades, moves/changes.

Release 4.1 introduces licensing on the VSP 4000 platform with a premier license being required for Layer 3 VSNs and MACsec features.

There are two types of Premier licenses:

- Support for Layer 3 VSNs only
- Support for Layer 3 VSNs and MACsec

All other features that are part of 4.1 are not licensed.

For more information, see [Feature licensing](#) on page 36.

For customers that would like to trial premier features prior to purchasing a premier license, there are there are two types of PLDS Premier trial licenses that will permit use of premier features for a 60 day period:

- Support for Layer 3 VSNs only
- Support for Layer 3 VSNs and MACsec

The PLDS Premier trial license is generated using the system MAC address of a switch and can only be generated and used once for a given MAC address. After the expiry of the 60 day trial period, you will see messages on the console and in the alarms database that the license has expired. If you restart the system after the license expiration, the Premier features will not be loaded even if they are in the saved configuration. If you purchase a Premier license, you must obtain and install a license file. For more information about how to generate a license file, see *Getting Started with Avaya PLDS for Avaya Networking Products*, NN46199-300.

For more information about PLDS and installing a license file, see *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600

SFP+ transceivers

Release 4.1 introduces support for the following SFP+ transceivers.

Transceiver	Description	Part number
10GBASE-LR/LW (-5 °C to +85 °C)	1310 nm SMF with a range up to 10 km	AA1403011-E6HT
10GBASE-SR/SW (0 °C to +85 °C)	850 nm with a range up to 400 m (OM4)	AA1403015-E6HT

For more information, see *Installing Transceivers and Optical components on Avaya Virtual Services Platform 4000 Series*, NN46251-301.

Simplified IGMP Access-Policy configuration

Release 4.1 supports simplified IGMP Access-Policy configuration, without having to specify VLAN IP subnet on the command line.

For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series*, NN46251–504.

Transparent-UNI with virtual IST support

Release 4.1 supports T-UNI with vIST support.

For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series*, NN46251-510.

SSL certificate management

This release adds support to manage an SSL certificate on the switch. You can install or remove a certificate, and configure the expiration time for a new certificate. This release also changes the default size of the certificate key length from 1,024 bits to 2,048 bits. The change in default size applies only to a new certificate; an existing certificate remains unchanged.

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

Overview of features and hardware models by release

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

* Note:

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

Features for Releases 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 release				
	4.1	4.0	3.1	3.0.1	3.0
Operations and Management					
spbm-config-mode boot flag For more information, see <i>Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series</i> , NN46251–504.	X				
Domain Name Service (DNS) client (IPv6) For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251–600.	X				
Extensible Authentication Protocol over LAN (EAPoL)	X				

Table continues...

Features	New in release				
	4.1	4.0	3.1	3.0.1	3.0
For more information, see <i>Avaya Virtual Services Platform 4000 Series Security</i> , NN46251–601.					
RADIUS (IPv6) For more information, see <i>Avaya Virtual Services Platform 4000 Series Security</i> , NN46251–601.	X				
Secure Shell (SSH) server (IPv6) For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251–600.	X				
Simple Network Management Protocol (SNMP) (IPv6) For more information, see <i>Avaya Virtual Services Platform 4000 Series Security</i> , NN46251–601.	X				
Telnet client and server (IPv6) For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251–600.	X				
Trivial File Transfer Protocol (TFTP) Client and Server (IPv6) For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251–600.	X				
Media Access Control Security (MACsec) For more information, see <i>Avaya Virtual Services Platform 4000 Series Security</i> , NN46251–601. * Note: The MACsec feature is supported only on the VSP 4450GSX-PWR +.		X			
TACACS+ For more information, see <i>Avaya Virtual Services Platform 4000 Series Security</i> , NN46251–601.		X			
IEEE 802.1ag Connectivity Fault Management (CFM) (For both BVLAN and CVLAN) For more information, see <i>Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series</i> , NN46251–510.			X		
Avaya CLI (ACLI) For more information, see <i>Avaya Virtual Services Platform 4000 Series Command Line Reference Guide</i> , NN46251–104.					X
Domain Name Service (DNS) client (IPv4) For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251–600.					X

Table continues...

Features	New in release				
	4.1	4.0	3.1	3.0.1	3.0
Enterprise Device Manager (EDM) For more information, see Avaya Configuration and Orchestration Manager (COM) documentation, http://support.avaya.com .					X
Flight Recorder for system health monitoring For more information, see <i>Avaya Virtual Services Platform 4000 Series Troubleshooting</i> , NN46251-700.					X
FTP Server For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251-600.					X
HTTP and HTTPS EDM management For more information, see <i>Avaya Virtual Services Platform 4000 Series User Interface Fundamentals</i> , NN46251-103.					X
IEEE 802.1ax (802.3ad) Link Aggregation Control Protocol (LACP) For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – Link Aggregation and MLT</i> , NN46251-503.					X
Key Health Indicator (KHI) For more information, see <i>Avaya Virtual Services Platform 4000 Series Fault Management</i> , NN46251-702.					X
RADIUS (IPv4) For more information, see <i>Avaya Virtual Services Platform 4000 Series Security</i> , NN46251-601.					X
Secure Copy server For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251-600.					X
Secure Shell (SSH) v1 and v2 server/client (IPv4) For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251-600.					X
Secure Sockets Layer (SSL) certificate management For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251-600.	X				
Simple Loop Prevention Protocol (SLPP) For more information, see <i>Network Design Reference for Avaya Virtual Services Platform 4000 Series</i> , NN46251-200.					X
Simple Network Management Protocol (SNMP) (IPv4) For more information, see <i>Avaya Virtual Services Platform 4000 Series Security</i> , NN46251-601.					X

Table continues...

Features	New in release				
	4.1	4.0	3.1	3.0.1	3.0
Telnet client and server (IPv4) For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251–600.					X
Trivial File Transfer Protocol (TFTP) Client and Server (IPv4) For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251–600.					X
Virtual LACP (VLACP) End-to-End connectivity check For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – Link Aggregation and MLT</i> , NN46251-503.					X
9600 bytes Jumbo packet support For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251–600.					X
Layer 2					
Avaya VENA Switch Cluster (Multi-Chassis LAG) • Virtual Inter-Switch Trunk (vIST) For more information, see <i>Configuring Link Aggregation and MLT on Avaya Virtual Services Platform 4000 Series</i> , NN46251-503.	X				
IEEE 802.1d Mac Bridges Spanning Tree For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – VLANs and Spanning Tree</i> , NN46251–500.					X
IEEE 802.1s MSTP For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – VLANs and Spanning Tree</i> , NN46251–500.					X
IEEE 802.1w RSTP For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – VLANs and Spanning Tree</i> , NN46251–500.					X
MLT (Multilink trunking) For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – Link Aggregation and MLT</i> , NN46251-503.					X
Avaya VENA Fabric Connect					
All Avaya Fabric Connect services with Avaya VENA Switch Cluster For more information, see <i>Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series</i> , NN46251-510.	X				
IS-IS accept policies. For more information, see <i>Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series</i> , NN46251-510.	X				

Table continues...

Features	New in release				
	4.1	4.0	3.1	3.0.1	3.0
IPv6 Inter-VSN Routing For more information, see <i>Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series</i> , NN46251–510.	X				
<code>run spbm</code> installation script For more information, see <i>Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series</i> , NN46251–510.	X				
<code>vms endura</code> automation script For more information, see <i>Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series</i> , NN46251–510.	X				
IP Multicast over SBPM For more information, see <i>Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series</i> , NN46251–510.			X		
Transparent UNI (T-UNI) For more information, see <i>Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series</i> , NN46251–510.			X		
E-Tree configuration For more information, see <i>Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series</i> , NN46251–510.				X	
IEEE 802.1aq Shortest Path Bridging MACinMAC (SPBM) For more information, see <i>Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series</i> , NN46251–510.					X
Inter-VSN Routing For more information, see <i>Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series</i> , NN46251–510.					X
Layer 2 Virtual Service Network (VSN) For more information, see <i>Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series</i> , NN46251–510.					X
Layer 3 Virtual Service Network (VSN) For more information, see <i>Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series</i> , NN46251–510.					X
Layer 3 IPv4 and IPv6 Routing Services					
IPv6 (OSPFv3, VRRP, RSMLT, DHCP Relay, IPv4 in IPv6 tunnels) For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – IPv6 Routing</i> , NN46251-511.	X				
Layer 3 Switch Cluster (Routed SMLT) with Virtual Inter-Switch Trunk (vIST)	X				

Table continues...

Features	New in release				
	4.1	4.0	3.1	3.0.1	3.0
For more information, see <i>Configuring Link Aggregation and MLT on Avaya Virtual Services Platform 4000 Series</i> , NN46251-503.					
Layer 3 Switch Cluster (Routed SMLT) with Simplified vIST For more information, see <i>Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series</i> , NN46251-504.	X				
Protocol Independent Multicast–Sparse Mode (PIM-SM), PIM-Source Specific Mode (PIM-SSM) For more information, see <i>Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series</i> , NN46251-504	X				
Neighbor Discovery (ND) (IPv6) For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – IPv6 Routing</i> , NN46251-511.	X				
Autogenerated CFM MEP and MIP levels For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – OSPF and RIP</i> , NN46251-506.			X		
BGP services For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – BGP</i> , NN46251-507.			X		
OSPF and RIP For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – OSPF and RIP</i> , NN46251-506.			X		
ARP and RARP For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – IP Routing</i> , NN46251-505.					X
DHCP Relay agent For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – IP Routing</i> , NN46251-505.					X
DHCP Relay Option 82 For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – IP Routing</i> , NN46251-505.					X
Equal Cost MultiPath (ECMP) For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – IP Routing</i> , NN46251-505.					X
IP Static routes For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – IP Routing</i> , NN46251-505.					X
Virtual Router Redundancy Protocol (VRRP)					X

Table continues...

Features	New in release				
	4.1	4.0	3.1	3.0.1	3.0
For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – IP Routing</i> , NN46251-505.					
Virtual Routing Forwarding (VRF) Lite (24 instances) For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – IP Routing</i> , NN46251-505.					X
VRRP BackupMaster For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – IP Routing</i> , NN46251-505.					X
Quality-of-Service and filtering					
Service Level Agreement Monitor For more information, see <i>Performance Management of Avaya Virtual Services Platform 4000 Series</i> , NN46251-701.		X			
Private VLAN For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – VLANs and Spanning Tree</i> , NN46251-500.				X	
Diffserv framework For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – QoS and ACL Based Traffic Filtering</i> , NN46251-502.					X
Egress port shapers For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – QoS and ACL Based Traffic Filtering</i> , NN46251-502.					X
IEEE 802.1p/q Virtual LAN For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – VLANs and Spanning Tree</i> , NN46251-500.					X
Ingress port policers For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – QoS and ACL Based Traffic Filtering</i> , NN46251-502.					X
IP Brouter port For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – VLANs and Spanning Tree</i> , NN46251-500.					X
Line Rate Ingress and Egress Port and VLAN ACLs for Layer 2 to Layer 4 For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – QoS and ACL Based Traffic Filtering</i> , NN46251-502.					X
Port and Protocol-based VLANs For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – VLANs and Spanning Tree</i> , NN46251-500.					X

Table continues...

Features	New in release				
	4.1	4.0	3.1	3.0.1	3.0
Port Mirroring ingress and egress For more information, see <i>Avaya Virtual Services Platform 4000 Series Troubleshooting</i> , 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 * Note: The DC model is not supported in Release 4.1. This model will be supported in Release 4.1.1.	EC4400004-E6	4.0.50
TAA-compliant VSP 4450GSX-PWR+	EC4400A05-E6GS EC4400B05-E6GS EC4400C05-E6GS EC4400D05-E6GS EC4400E05-E6GS EC4400F05-E6GS	4.0.50
VSP 4450GTX-HT-PWR+	EC4400A03-E6 EC4400E03-E6	4.0.40
VSP 4450GSX-PWR+	EC4400A05-E6 EC4400B05-E6 EC4400C05-E6 EC4400D05-E6 EC4400E05-E6 EC4400F05-E6	4.x
VSP 4850GTS	EC4800A78-E6 EC4800B78-E6 EC4800C78-E6 EC4800D78-E6 EC4800E78-E6 EC4800F78-E6	3.x

Table continues...

Model	Part number	Release
VSP 4850GTS-PWR+	EC4800A88-E6	3.x
	EC4800B88-E6	
	EC4800C88-E6	
	EC4800D88-E6	
	EC4800E88-E6	
	EC4800F88-E6	
VSP 4850GTS DC	EC4800078-E6	3.x

For more information about hardware models, see [Hardware compatibility](#) on page 25, *Installing Avaya Virtual Services Platform4450GTX-HT-PWR+Switch*, NN46251–304, and *Installing Avaya Virtual Services Platform4450GSX-PWR+Switch*, NN46251–307.

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 Release 4.1:

Feature	VSP 4000	VSP 8000
CMAC — CFM	Supported	Not Supported
COM	*	*
VMS Endura scripts	Supported	Not Supported
FDB protect by port	Supported	Not Supported
NLB Unicast	Not Supported	Supported
QoS	Supported	Supported with exceptions: <ul style="list-style-type: none"> • Classification does not have routed packet classification • No ingress policer- Uses ingress port rate limiting instead
Transparent UNI	Supported	Not Supported

* COM does not currently support the VSP 4000 or VSP 8000 for Release 4.1, but support is planned in a future COM release. The EDM plug-in (COM war file) is provided with Release 4.1 software so that it will be available to you when COM supports Release 4.1.

Other Changes

There are no other changes in this document that are not feature-related.

Chapter 3: Important notices

This section describes the supported hardware and software scaling capabilities of the Avaya Virtual Services Platform 4000 and provides important information for this release.

Hardware compatibility

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

*** Note:**

For information about transceivers and the list of supported SFP and SFP+ transceivers, see *Installing Transceivers and Optical components on Avaya Virtual Services Platform 4000*, NN46251–301.

Table 1: Hardware

Release	VSP 4000 model	Description	Part number
3.0	VSP 4850GTS	<ul style="list-style-type: none">• 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	EC4800A78-E6
		<ul style="list-style-type: none">• Same content as EC4800A78-E6 with a EU power cord.	EC4800B78-E6
		<ul style="list-style-type: none">• Same content as EC4800A78-E6 with a UK power cord.	EC4800C78-E6
		<ul style="list-style-type: none">• Same content as EC4800A78-E6 with a JP power cord.	EC4800D78-E6
		<ul style="list-style-type: none">• Same content as EC4800A78-E6 with a NA power cord.	EC4800E78-E6
		<ul style="list-style-type: none">• Same content as EC4800A78-E6 with a EU power cord.	EC4800F78-E6

Table continues...

Release	VSP 4000 model	Description	Part number
3.0	VSP 4850GTS-PWR+	<ul style="list-style-type: none"> • 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 	EC4800A88-E6
		<ul style="list-style-type: none"> • Same content as EC4800A88-E6 with a EU power cord. 	EC4800B88-E6
		<ul style="list-style-type: none"> • Same content as EC4800A88-E6 with a UK power cord. 	EC4800C88-E6
		<ul style="list-style-type: none"> • Same content as EC4800A88-E6 with a JP power cord. 	EC4800D88-E6
		<ul style="list-style-type: none"> • Same content as EC4800A88-E6 with a NA power cord. 	EC4800E88-E6
		<ul style="list-style-type: none"> • Same content a EC4800A88-E6 with a AU power cord. 	EC4800F88-E6
3.0	VSP 4850GTS DC	<ul style="list-style-type: none"> • 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+	<ul style="list-style-type: none"> • 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 	EC4400A05-E6
		<ul style="list-style-type: none"> • Same content as EC4400A05-E6 with a EU power cord. 	EC4400B05-E6
		<ul style="list-style-type: none"> • Same content as EC4400A05-E6 with a UK power cord. 	EC4400C05-E6
		<ul style="list-style-type: none"> • Same content as EC4400A05-E6 with a JP power cord. 	EC4400D05-E6
		<ul style="list-style-type: none"> • Same content as EC4400A05-E6 with a NA power cord. 	EC4400E05-E6
		<ul style="list-style-type: none"> • Same content a EC4400A05-E6 with a AU power cord. 	EC4400F05-E6

Table continues...

Release	VSP 4000 model	Description	Part number
4.0.40	VSP 4450GTX-HT-PWR+	<ul style="list-style-type: none"> 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
		<ul style="list-style-type: none"> Same content as EC4400A03-E6 with a NA power cord. 	EC4400E03-E6
4.0.50	TAA-compliant VSP 4450GSX-PWR+	<ul style="list-style-type: none"> 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 	EC4400A05-E6GS
		<ul style="list-style-type: none"> Same content as EC4400A05-E6 with a EU power cord. 	EC4400B05-E6GS
		<ul style="list-style-type: none"> Same content as EC4400A05-E6 with a UK power cord. 	EC4400C05-E6GS
		<ul style="list-style-type: none"> Same content as EC4400A05-E6 with a JP power cord. 	EC4400D05-E6GS
		<ul style="list-style-type: none"> Same content as EC4400A05-E6 with a NA power cord. 	EC4400E05-E6GS
		<ul style="list-style-type: none"> Same content a EC4400A05-E6 with a AU power cord. 	EC4400F05-E6GS

*** Note:**

The VSP 4450GSX-DC model is not supported in Release 4.1. This model will be supported in Release 4.1.1.

Platform 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 2: 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*
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
<p>*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:</p> <p>“A”: No power cord included.</p> <p>“B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden.</p> <p>“C”: Includes power cord commonly used in the United Kingdom and Ireland.</p> <p>“D”: Includes power cord commonly used in Japan.</p> <p>“E”: Includes North American power cord.</p> <p>“F”: Includes Australian power cord.</p>		

Software scaling capabilities

This chapter lists software scaling capabilities of Avaya Virtual Services Platform 4000 Series.

Table 3: Software scaling capabilities

	Maximum number supported
Layer 2	
MAC table size (without SPBM)	32,000

Table continues...

	Maximum number supported
MAC table size (with SPBM)	16,000
Port-based VLANs	4,059
Protocol-based VLANs (IPv6 only)	1
Multiple Spanning Tree Protocol (MSTP) instances	12
Rapid Spanning Tree Protocol (RSTP) instances	1
LACP aggregators	24
Ports per LACP aggregator	16 (8 active and 8 standby)
MultiLink Trunking (MLT) groups	24
Ports per MLT group	8
SLPP VLANs	128
VLACP interfaces	50
Layer 3	
IPv4 VRF instances	24
IP interfaces (IPv4 or IPv6)	256
Routed Split Multi-Link Trunking (RSMLT) interfaces (IPv4 or IPv6)	252
VRRP interfaces (IPv4 or IPv6)	64
VRRP interfaces with fast timers (200 ms) (IPv4 or IPv6)	24
IPv4 Circuitless IP interfaces	64
IPv6 Circuitless IP interfaces	1
IPv4 Address Resolution Protocol (ARP) table	6,000
IPv6 neighbor table	4,000
IPv4 static ARP entries	200 for each VRF 1,000 for each switch
IPv6 static neighbor records	128
IPv4 route table size	16,000
IPv6 route table size (prefix length < 64 bits)	8,000
IPv6 route table size (prefix length > 64 bits)	256
IPv6 6in4 configured tunnels	254
IPv4 Static routes	1,000 for each VRF 1,000 for each switch
IPv6 static routes	1,000
ECMP groups/Paths per group	500 groups with a maximum of 4 ECMP paths per group
RIP interfaces	24

Table continues...

	Maximum number supported
OSPF v2/v3 interfaces	48 (24 passive)
OSPF v2/v3 neighbors (adjacencies)	24
OSPF areas	12 for each VRF 64 for each switch
e-BGP peers	12
IPv4 RIP routes	2,000 for each VRF 2,000 for each switch
IPv4 OSPF routes	16,000 for each VRF 16,000 for each switch
IPv4 e-BGP routes	16,000 for each VRF 16,000 for each switch
IPv4 shortcut routes	16,000 for each VRF 16,000 for each switch
IPv6 OSPFv3 routes – GRT only	8,000
IPv6 shortcut routes – GRT only	8,000
IPv4 route policies	500 for each VRF 5,000 for each switch
IP Multicast	
IGMP interfaces	4059
PIM interfaces	Active – 128 Passive – 256
PIM neighbors (GRT only)	128
PIM-SSM static channels	512
Multicast receivers or IGMP joins (per switch)	1000
Multicast senders (per switch)	1000
Total multicast routes (per switch)	4000
Static multicast routes	512
Multicast enabled Layer 2 VSNs	1,000
Multicast enabled Layer 3 VSNs	24
SPBM	
SPBM enabled switches per region (BEB + BCB)	2,000
Service endpoint switches (BEBs) per I-SID	2,000
IS-IS interfaces	50
IS-IS adjacencies	50

Table continues...

	Maximum number supported
Layer 2 VSNs per switch (VLANs mapped to I-SID)	1,000
Layer 3 VSNs per switch (VRF mapped to I-SID)	24
Transparent-UNI services per switch (Port mapped to I-SID)	48
E-Tree	
Number of private VLANs	1,000
Filters and QoS	
Total IPv4 Ingress rules (Port/VLAN based, Security/QoS filters)	1530
Total IPv4 Egress rules (Port based, Security filters)	254
Total IPv6 Ingress rules (Port/VLAN based, Security/QoS filters)	256
Diagnostics	
Mirrored ports	49
OAM	
FTP sessions (IPv4 or IPv6)	4 each
Rlogin sessions (IPv4 or IPv6)	8 each
SSH sessions (IPv4 or IPv6)	8 shared (any combination of IPv4 and IPv6 up to 8)
Telnet sessions (IPv4 or IPv6)	8 each

File names for release 4.1

This section describes the Avaya Virtual Services Platform 4000 software files.

Software files

The following table provides the details of the Virtual Services Platform 4000 software files. File sizes are approximate.

Table 4: Software files

Module or file type	Description	File name	File size (bytes)
Standard Runtime Software Image	Standard image for Avaya Virtual Services Platform 4000 Series.	VSP4K.4.1.0.0.tgz	88,885,328

Table continues...

Module or file type	Description	File name	File size (bytes)
Encryption Module	Encryption module for Avaya Virtual Services Platform 4000 Series.	VSP4K.4.1.0.0_modules.tgz	82,069

Table 5: Enterprise Device Manager Help files

Module or file type	Description	File name	File size (bytes)
Enterprise Device Manager Help Files	Enterprise Device Manager Help files for Avaya Virtual Services Platform 4000 Series.	VSP4000v410_HELP_EDM_gzip.zip	2,773,914

Open Source software files

The following table gives the details of the Open Source software files distributed with the Virtual Services Platform 4000 software.

Table 6: Open Source software files

File name	Description	Size
VSP4K.4.1.0.0_oss-notice.html	Master copyright file. This file is located in the Licenses directory.	414,245
VSP4K.4.1.0.0_OpenSource.zip	Open source base software for Virtual Services Platform 4000 Release 4.1.	95,859,832

You can download Avaya Virtual Services Platform 4000 software and files, including MIB files, from the Avaya Support Portal at www.avaya.com/support. Click **Downloads**.

 **Caution:**

To download the software and files, use one of the following browsers: IE 9 or greater, or Mozilla Firefox.

 **Important:**

After you download the software, calculate and verify the md5 checksum. To calculate and verify the md5 checksum on a Unix or Linux machine, see [Calculating and verifying the md5 checksum on a switch](#) on page 33 and [Calculating and verifying the md5 checksum on a client](#) on page 34. On a Windows machine, use the appropriate Windows utility that is supported on your Windows version.

The Open Source license text for the VSP 4000 is included on the VSP 4000 product and is accessible via the Command Line Interface by typing the following: `more release/4.1.0.0.GA/release/oss-notice.txt`.

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 VSP8200.4.1.0.0_edoc.tar
d000965876dee2387f1ca59cf081b9d6 VSP8200.4.1.0.0_mib.txt
897303242c30fd944d435a4517f1b3f5 VSP8200.4.1.0.0_mib.zip
2fbd5eab1c450d1f5feae865b9e02baf VSP8200.4.1.0.0_modules.tgz
a9d6d18a979b233076d2d3de0e152fc5 VSP8200.4.1.0.0_OpenSource.zip
8ce39996a131de0b836db629b5362a8a VSP8200.4.1.0.0_oss-notice.html
80bfe69d89c831543623aaad861f12aa VSP8200.4.1.0.0.tgz
a63a1d911450ef2f034d3d55e576eca0 VSP8200v4.1.0.0.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 VSP8200.4.1.0.0.tgz
-rw-r--r-- 1 0 0 44208471 Dec 8 08:19 VSP8200.4.1.0.0.tgz
Switch:1>md5 VSP8200.4.0.0.0.tgz
MD5 (VSP8200.4.1.0.0.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.4.1.0.0.tgz
02c7ee0570a414becf8ebb928b398f51 VSP4K.4.1.0.0.tgz
```

View the md5 checksum of the software suite:

```
$ more VSP4K.4.1.0.0.md5
285620fdc1ce5ccd8e5d3460790c9fe1 VSP4000v4.1.0.0.zip
a04e7c7cef660bb412598574516c548f VSP4000v4100_HELP_EDM_gzip.zip
ac3d9cef0ac2e334cf94799ff0bdd13b VSP4K.4.1.0.0_edoc.tar
29fa2aa4b985b39843d980bb9d242110 VSP4K.4.1.0.0_mib_sup.txt
c5f84beaf2927d937fcbe9dd4d4c7795 VSP4K.4.1.0.0_mib.txt
ce460168411f21abf7ccd8722866574c VSP4K.4.1.0.0_mib.zip
1ed7d4cda8b6f0aaf2cc6d3588395e88 VSP4K.4.1.0.0_modules.tgz
1464f23c99298b80734f8e7fa32e65aa VSP4K.4.1.0.0_OpenSource.zip
945f84cb213f84a33920bf31c091c09f VSP4K.4.1.0.0_oss-notice.html
02c7ee0570a414becf8ebb928b398f51 VSP4K.4.1.0.0.tgz
```

Important information and restrictions

This section contains important information and restrictions you must consider before you use the Avaya Virtual Services Platform 4000.

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.

Supported browsers

Virtual Services Platform 4000 supports the following browsers to access the 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 VSP 4000 system, 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 *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600.

Feature licensing

Starting with Release 4.1, VSP 4000 feature licensing is transitioned to Product Licensing & Delivery System (PLDS) with the earlier three tier framework changed to a two tier framework. The two tier framework includes the following license levels.

- Base software license
- Premier software license

Note:

For existing VSP 4000 deployments with licenses installed, the previously purchased and installed licenses will continue to operate when the switches are upgraded to Release 4.1 and higher. Because advanced features are part of the Base software license in Release 4.1, the previously installed Advanced licenses will be ignored and those features will continue to operate with the Base license.

Important:

To prevent licensing issues in the unlikely event of a software downgrade to Release 4.0 or earlier, do not uninstall the existing Advance license on these switches so that there is no impact to the licensed features in earlier releases.

For more information on the PLDS licensing, see *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600.

Base software license

The Base software license is provided free of charge with the purchase of the VSP 4000 hardware. You do not require a license file to unlock the base features.

The following features are included under the Base software licence:

- Layer 2 Features:
 - Core Layer 2 Switching, ACLs, Policers, Shapers
 - IEEE 802.1D/w/s, IEEE 802.1p/Q
 - MLT/LACP
 - SPB Base functionality
 - SPB Layer 2 VSNs (including Multicast)
 - SPB IEEE 802.1ag CFM
 - E-Tree/Private VLANs
 - Transparent UNI
 - Switch Clustering with virtual IST (SMLT with vIST)
- IPv4 and IPv6 routing features:
 - GRT IP Routing
 - Static routing, RIP, OSPF v2/v3, BGP

- VRRP v2/v3
- DHCP Relay
- Configured Tunnels (6 in 4)
- ISIS Accept Policies for IPv4 Routing
- SPB IP shortcuts (IPv4 & IPv6)
- SPB Inter-VSN Routing
- Routed Switch Clustering with virtual IST (R-SMLT with vIST)
- IP Multicast features:
 - IGMP
 - MLD v1/v2 host mode
 - PIM SM/SSM
 - IP Multicast over Fabric Connect
- Layer 3 Virtualization features:
 - IPv4 VRFs

Premier software license

A separate Premier software license is required to enable each of the following Layer 3 virtualization features on VSP 4000.

- SPB Layer 3 VSNs (including Multicast)
- IEEE 802.1AE MACsec

To trial premier features prior to purchasing a premier license, there are there are two types of PLDS Premier trial licenses that will permit use of premier features for a 60 day period.

The PLDS Premier trial license is generated using the system MAC address of a switch and can only be generated and used once for a given MAC address. After the expiry of the 60 day trial period, you will see messages on the console and in the alarms database that the license has expired. If you restart the system after the license expiration, the Premier features will not be loaded even if they are in the saved configuration. 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 *Getting Started with Avaya PLDS for Avaya Networking Products*, NN46199-300.

The various Premier licenses supported on Virtual Services Platform 4000 are as follows:

- PLDS Premier License
- PLDS Premier License with MACsec
- PLDS Premier Trial License
- PLDS Premier Trial License with MACsec
- Premier to Premier with MACsec Uplift License

Combination ports

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.

SFP and SFP+ ports and use of lower speed transceivers

- The SFP+ ports only operate at 1G and 10G speeds, so the 1000Base-T SFP transceiver (AA1419043-E6) will only operate at 1000Mbps when used in the SFP+ ports.
- The 100BASE-FX SFP transceiver (AA1419074-E6) is only supported on 1 Gigabit Ethernet SFP ports on VSP 4000.

Shutting down VSP 4000

Use the following procedure to shut down VSP 4000.

 **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 the Priviledged EXEC configuration mode.

```
enable
```

2. Shut down VSP 4000:

```
sys shutdown
```

Example

```
VSP-4450GSX-PWR+:1>enable
```

```
VSP-4450GSX-PWR+:1#sys shutdown
```

```
Are you sure you want shutdown the system? Y/N (y/n) ? y
```

```
CP1 [03/24/14 18:39:04.932:UTC] 0x00010813 00000000 GlobalRouter HW INFO
System shutdown initiated from CLI
```

```
CP1 [03/24/14 18:39:06.000] LifeCycle: INFO: Stopping all processes
```

```
CP1 [03/24/14 18:39:08.000] LifeCycle: INFO: All processes have stopped
```

```
CP1 [03/24/14 18:39:08.000] 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
```

```
cat: can't open '/proc/mtd': No such file or directory
```

```
cat: can't open '/proc/mtd': No such file or directory
```

```
Stopping vsp...
```

```
mount: no /proc/mounts
```

```
mount: can't find /mnt/cfgfs/ in /etc/fstab
```

```
/etc/rc0.d/K25vsp: line 441: /mnt/cfgfs/timestamp: Read-only file system
```

```
umount: can't open '/proc/mounts'
```

```
sed: /proc/mounts: No such file or directory
```

```
sed: /proc/mounts: No such file or directory
```

Important notices

```
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...
hwclock: can't open '/dev/misc/rtc': No such file or directory
/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...
[695413.959234] Power down.
[695413.989531] System Halted, OK to turn off power
```

Interoperability notes for VSP 4000 or VSP 8000 connecting with ERS 5650

ERS 5650 operation causes a temporary loop that restarts the LACP-SMLT ports on the VSP 4000 or VSP 8000. This loop can shut down the LACP-SMLT port if SLPP is running on the port.

To prevent shutdown of the port on the switch, avoid using SLPP on LACP-SMLT ports.

Note:

When using Avaya ERS 5000 Series switches as SMLT edge devices with LACP-SMLT, use Advance LACP port mode on these switches to avoid the loop.

Chapter 4: Software Upgrade

Image upgrade fundamentals

This section details what you must know to upgrade the Virtual Services Platform 4000.

Upgrades

Install new software upgrades to add functionality to the Virtual Services Platform 4000. 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 Virtual Services Platform 4000 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 Virtual Services Platform 4000, 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

VSP 4000 software use a standardized dot notation format. This standardized format is as follows:

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.4.0.40.0.tgz** denotes a software image for the VSP 4K product with a major release version of 4, a minor release version of 0, a maintenance release version of 40 and a maintenance release update version of 0. TGZ is the file extension. Similarly, the image file name **VSP4K.4.1.0.0.tgz** denotes a software image for the VSP 4K product with a major release version of 4, a minor release version of 1, a maintenance release version of 0 and a maintenance release update version of 0.

Interfaces

You can apply upgrades and add encryption modules to the Virtual Services Platform 4000 using the Avaya Command Line Interface (ACLI).

For more information about ACLI, see *User Interface Fundamentals for Avaya Virtual Services Platform 4000 Series*, NN46251-103.

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.

Upgrading the software

Perform this procedure to upgrade the software on the Avaya VSP 4000 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.

Important:

Software upgrade is supported on the VSP 4850GTS, VSP 4850GTS-PWR+, VSP 4450GSX-PWR+ series, and VSP4450GTS-HT-PWR+. The VSP 4850GTS and VSP 4850GTS-PWR+

support upgrade from Releases 3.0, 3.0.1, 3.1, and 4.0 to Release 4.1. The VSP 4450GSX-PWR+ series supports upgrade from Release 4.0, 4.0.40, and 4.0.50 to Release 4.1. The VSP4450GTS-HT-PWR+ supports upgrade from Release 4.0.40 to Release 4.1.

*** Note:**

There is a limit of six software releases that can be stored on the VSP 4000 system. If you have six releases already stored on the VSP 4000 system, 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 47.

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

Upgrade path	Support
Upgrade from 3.0 to 4.1	Supported
Upgrade from 3.0.1 to 4.1	Supported
Upgrade from 3.1 to 4.1	Supported
Upgrade from 4.0 to 4.1	Supported

Supported upgrade paths on the VSP 4450GSX-PWR+ series and VSP4450GTS-HT-PWR+:

Upgrade path	Support
Upgrade from 4.0 to 4.1	Supported
Upgrade from 4.0.40 to 4.1	Supported
Upgrade from 4.0.50 to 4.1	Supported

Before you begin

- Back up the configuration files.
- Upload the file with the new software release to the VSP 4000 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. Enable FTP:

```
boot config flag ftpd
```

3. Enter Privileged EXEC configuration mode by exiting the Global Configuration mode.

```
exit
```

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

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

5. (Optional) To install encryption modules on the switch, extract the module files to the /intflash/release directory:

```
Software add-module [software version] [modules file name]
```

6. Install the image:

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

7. Restart the Virtual Services Platform 4000 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

```
VSP-4450GSX-PWR+:1>enable
```

```
VSP-4450GSX-PWR+:1#configure terminal
```

```
VSP-4450GSX-PWR+:1(config)#boot config flag ftpd
```

```
VSP-4450GSX-PWR+:1>exit
```

```
VSP-4450GSX-PWR+:1#software add VSP4K.4.1.0.0.tgz
```

```
VSP-4450GSX-PWR+:1#software add-modules 4.1.0.0.GA VSP4K.4.1.0.0_modules.tgz
```

```
VSP-4450GSX-PWR+:1#software activate VSP4000.4.1.0.0.GA
```

```
VSP-4450GSX-PWR+:1#reset
```

```
VSP-4450GSX-PWR+:1#show software
```

```
=====
                        software releases in /intflash/release/
=====
```

```
VSP4000.4.1.0.0.GA (Primary Release)
```

```
MP
```

```
UBOOT                vsp4k-10
KERNEL               2.6.32_int38
ROOTFS               2.6.32_int38
APPFS                VSP4K.4.1.0.0int031
AVAILABLE ENCRYPTION MODULES
No Modules Added
```

```
-----
Auto Commit          : enabled
Commit Timeout       : 10 minutes
```

```
VSP-4450GSX-PWR+:1#software commit
```

Verifying the upgrade

Verify your upgrade to ensure proper Avaya Virtual Services Platform 4000 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 Avaya Virtual Services Platform 4000 from the current trusted version to a previous release.

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 Virtual Services Platform 4000:

```
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 Avaya Virtual Services Platform 4000.

*** Note:**

There is a limit of six software releases that can be stored on the VSP 4000 system. If you have six releases already stored on the VSP 4000 system, then you will be prompted to remove one release before you can proceed with adding and activating a new software release.

For information about adding and activating a software release, see [Upgrading the software](#) on page 42.

Procedure

1. Enter Privileged EXEC configuration mode:

```
enable
```

2. Remove software:

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

Example

```
VSP-4450GSX-PWR+:1>enable
```

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

Chapter 5: Supported standards, RFCs, and MIBs

This chapter details the standards, request for comments (RFC), and Management Information Bases (MIB) that Avaya Virtual Services Platform 4000 Series supports.

Supported IEEE standards

The following table details the IEEE standards that Avaya Virtual Services Platform 4000 Series supports.

Table 7: Supported IEEE standards

IEEE standard	Description
802.1aq	Shortest Path Bridging (SPB)
802.1d	MAC bridges (Spanning Tree)
802.1ax	Link Aggregation Control Protocol (LACP)
802.1p	Virtual Local Area Network (VLAN) prioritization
802.1q	Virtual Local Area Network (VLAN) tagging
802.1s	Multiple Spanning Tree Protocol
802.1t	802.1D maintenance
802.1w-2001	Rapid Spanning Tree Protocol (RSTP)
802.1x-2001	Extensible Authentication Protocol Over Local Area Networks (EAPoL)
802.3 CSMA/CD Ethernet ISO/IEC 8802	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 8802-3
802.3ab	Gigabit Ethernet 1000BaseT 4 pair Category 5 (CAT5) Unshielded Twisted Pair (UTP)
802.1ae	MACsec
802.3ae	10 Gigabit Ethernet
802.3af and 802.3at	PoE – Power over Ethernet

Table continues...

IEEE standard	Description
802.3i	10BaseT
802.3u	100BaseT
802.3x	flow control
802.3z	Gigabit Ethernet

Supported RFCs

The following table and sections list the RFCs that Avaya Virtual Services Platform 4000 Series supports.

Table 8: Supported request for comments

Request for comment	Description
draft-grant-tacacs-02.txt	TACACS+ Protocol
RFC768	UDP Protocol
RFC791	Internet Protocol (IP)
RFC792	Internet Control Message Protocol (ICMP)
RFC793	Transmission Control Protocol (TCP)
RFC826	Address Resolution Protocol (ARP)
RFC854	Telnet protocol
RFC894	A standard for the Transmission of IP Datagrams over Ethernet Networks
RFC896	Congestion control in IP/TCP internetworks
RFC906	Bootstrap loading using TFTP
RFC950	Internet Standard Subnetting Procedure
RFC951	BootP
RFC959, RFC1350, and RFC2428	IPv6 FTP and TFTP client and server
RFC1027	Using ARP to implement transparent subnet gateways/Nortel Subnet-based VLAN
RFC1122	Requirements for Internet Hosts
RFC1155	Structure and Identification of Management Information for TCP/IP-based Internets
RFC1156	MIB for network management of TCP/IP
RFC1157	SNMP
RFC1212	Concise MIB definitions
RFC1215	Convention for defining traps for use with the SNMP

Table continues...

Request for comment	Description
RFC1256	ICMP Router Discovery
RFC1258	BSD Rlogin server
RFC1305	Network Time Protocol v3 Specification, Implementation and Analysis
RFC1340	Assigned Numbers
RFC1398	Ethernet MIB
RFC1442	Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1450	Management Information Base for v2 of the Simple Network Management Protocol (SNMPv2)
RFC1493	Definitions of Managed Objects for Bridges
RFC1519	Classless Interdomain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC1542	Clarifications and Extensions for the Bootstrap Protocol
RFC1591	DNS Client
RFC1650	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC1724	RIPv2 MIB extensions
RFC1771	Border Gateway Protocol 4 (BGP-4)
RFC1772	Application of Border Gateway Protocol (BGP) in the internet
RFC1812	Router requirements
RFC1866	Hypertext Markup Language version 2 (HTMLv2) protocol
RFC1907	Management Information Base of the Simple Network Management Protocol version 2 (SNMPv2)
RFC1930	Guidelines for creation, selection, and registration of an Autonomous System (AS)
RFC1981	Path MTU Discovery
RFC1997	BGP Communities Attribute
RFC1998	Defining BGP communities
RFC2068	Hypertext Transfer Protocol
RFC2096	IP Forwarding Table MIB
RFC2131	Dynamic Host Control Protocol (DHCP)
RFC2138	RADIUS Authentication
RFC2139	RADIUS Accounting

Table continues...

Request for comment	Description
RFC2233	Interfaces Group MIB using SMIv2
RFC2328	OSPFv2
RFC2385	TCP MD5 Signature Option
RFC2439	BGP Route Flap Damping
RFC2454	Management Information Base for the User Datagram Protocol (UDP)
RFC2460	IPv6 Basic Specification
RFC2464	Transmission of IPv6 packets over Ethernet networks
RFC2474 and RFC2475	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC2578	Structure of Management Information Version 2 (SMIv2)
RFC2597	Assured Forwarding PHB Group
RFC2598	An Expedited Forwarding PHB
RFC2616	IPv6 Hypertext Transfer Protocol 1.1
RFC2674	Bridges with Traffic MIB
RFC2740	OSPF for IPv6
RFC2851	Textual Conventions for Internet Network Addresses
RFC2874	DNS Extensions for IPv6
RFC2932	IPv4 Multicast Routing MIB
RFC2933	IGMP MIB
RFC2934	PIM MIB
RFC2918	Route Refresh Capability for BGP-4
RFC2992	Analysis of an Equal-Cost Multipath Algorithm
RFC3046	DHCP Option 82
RFC3162	RADIUS and IPv6
RFC3315	DHCPv6 client/server/relay
RFC3411, RFC3412, RFC3413, RFC3414, and RFC3415	SNMP over IPv6 networks (SNMPv3)
RFC3416	v2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC3513	Internet Protocol Version 6 (IPv6) Addressing Architecture
RFC3587	IPv6 Global Unicast Address Format
RFC3596	DNS Extensions to Support IP Version 6
RFC3621	PoE – Power over Ethernet

Table continues...

Request for comment	Description
RFC3768 and draft-ietf-vrrp-ipv6-spec-08.txt	IPv6 capable VRRP
RFC4007	IPv6 Scoped Address Architecture
RFC4087	IP Tunnel MIB
RFC4213	IPv6 configured tunnel If support for tunneling and dual stack is required, the device must support Basic Transition Mechanisms for IPv6 Hosts and Routers
RFC4250, RFC4251, RFC4252, RFC4253, RFC4254, RFC4255, and RFC4256	SSH server and client support
RFC4291	IPv6 Addressing Architecture
RFC4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC4861	IPv6 Neighbor discovery
RFC4862	IPv6 stateless address autoconfiguration (SLAAC)
RFC5308	Routing IPv6 with IS-IS
RFC6329	IS-IS Extensions supporting Shortest Path Bridging

Standard MIBs

The following table details the standard MIBs that Avaya Virtual Services Platform 4000 Series supports.

Table 9: Supported MIBs

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
Link Aggregation Control Protocol (LACP) (802.3ad)	802.3ad	ieee802-lag.mib
SecY Management Table (secYIfTable)	802.1ae	ieee8021ae.mib
Exensible Authentication Protocol Over Local Area Networks (EAPoL) (802.1x)	802.1x	ieee8021x.mib
Internet Assigned Numbers Authority (IANA) Interface Type	—	iana_if_type.mib
MIB for network management of Transfer Control Protocol/Internet	RFC1213	rfc1213.mib

Table continues...

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
Protocol (TCP/IP)-based Internet MIB2		
A convention for defining traps for use with SNMP	RFC1215	rfc1215.mib
RIP Version 2 MIB Extension	RFC1389	rfc1389.mib
Definitions of Managed Objects for the Ethernet-like Interface Types	RFC1643	rfc1643.mib
BGP-4 MIB using SMIv2	RFC1657	rfc1657.mib
Remote Network Monitoring Management Information Base	RFC1757	rfc1757.mib
OSPF MIB	RFC1850	rfc1850.mib
IPv6 MIB: TCP MIB	RFC2452	rfc2452.mib
IPv6 MIB: UDP MIB	RFC2454	rfc2454.mib
IPv6 MIB: Textual Conventions and General Group MIB	RFC2465	rfc2465.mib
IPv6 MIB: ICMPv6 Group (ICMPv6) MIB	RFC2466	rfc2466.mib
Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework	RFC2576	rfc2576.mib
Definitions of Managed Objects for the Virtual Router Redundancy Protocol	RFC2787	rfc2787.mib
Textual Conventions for Internet Network Addresses	RFC2851	rfc2851.mib
The Interface Group MIB	RFC2863	rfc2863.mib
Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations	RFC2925	rfc2925.mib
SNMPv3 (These Request For Comments (RFC) make some previously named RFCs obsolete)	RFC3411, RFC3412, RFC3413, RFC3414, RFC3415	rfc2571.mib, rfc2572.mib, rfc2573.mib, rfc2574.mib, rfc2575.mib
Textual Conventions for IPv6 Flow Label	RFC3595	ipv6_flow_label.mib
Definitions of Managed Power over Ethernet	RFC3621	rfc3621.mib
The Advanced Encryption Standard (AES) Cipher Algorithm	RFC3826	rfc3826.mib

Table continues...

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
in the SNMP User-based Security Model		
Management Information Base for the Transmission Control Protocol (TCP)	RFC4022	rfc4022.mib
IP Tunnel MIB	RFC4087	rfc4087.mib
Management Information Base for the User Datagram Protocol (UDP)	RFC4113	rfc4113.mib
Entity MIB	RFC4133	rfc4133.mib
Definitions of Managed Objects for Bridges	RFC4188	rfc4188.mib
Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions	RFC4363	p_bridge.mib and q_bridge.mib


Proprietary MIBs

The following table details the proprietary MIBs that Avaya Virtual Services Platform 4000 Series supports.

Table 10: Proprietary MIBs

Proprietary MIB name	File name
Avaya IGMP MIB	rfc_igmp.mib
Avaya IP Multicast MIB	ipmroute_rcc.mib
Avaya MIB definitions	wf_com.mib
Avaya PIM MIB	pim-rcc.mib
Avaya RSTP/MSTP proprietary MIBs	nnrst000.mib, nnmst000.mib
Avaya SLA Monitor Agent MIB	slamon.mib
Other SynOptics definitions	s5114roo.mib
Other SynOptics definitions	s5emt103.mib
Other SynOptics definitions	s5tcs112.mib
Other SynOptics definition for Combo Ports	s5ifx.mib
Other SynOptics definition for PoE	bayStackPethExt.mib

Table continues...

Proprietary MIB name	File name
Rapid City MIB  Note: The MACsec tables, namely, rcMACSecCATable and rcMACSecIfConfigTable are a part of the Rapid City MIB.	rapid_city.mib
SynOptics Root MIB	synro.mib

Chapter 6: Known issues and limitations

This section details the known issues and limitations of the Avaya Virtual Services Platform 4000. Where appropriate, use the workarounds provided.

Known issues in release 4.1

The following sections identify the known issues in release 4.1 of the Avaya Virtual Services Platform 4000.

Device related issues

Table 11: Known issues

Issue number	Description	Workaround
wi01111785	<p>Internal QoS remapping with filters does not work for certain UDP destination ports.</p> <p>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.</p>	<p>The control packets received from the ingress port include the following:</p> <ul style="list-style-type: none">• 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
wi01134468	<p>On a T-UNI port with Layer 2 untrusted configuration, the internal QoS of the traffic flow is derived from the .1p bits of the ingress tagged traffic.</p> <p>If incoming client packets are tagged, the VSP 4000 system always derives the internal priority queue from the 802.1p tag.</p>	None
wi01134509	On a T-UNI port, with incoming untagged traffic, the internal QoS level of the traffic	None

Table continues...

Issue number	Description	Workaround
	<p>flow is set to 0, irrespective of the Layer 2 Trust configuration on the port.</p> <p>If incoming client packets are untagged, the internal priority queue of the VSP 4000 is always the best-effort queue.</p>	
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 Layer 2 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	<p>The <code>metric</code> field in the <code>redistribute</code> command is not supported for inter-VRF redistributed routes.</p> <p>This impacts only inter-VRF metric settings. It does not impact inter-VRF route filtering.</p>	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 Layer 2 Trusted with Layer 3 Untrusted and Diffserv disabled.	<p>None</p> <p>There is no impact to packet processing. The issue is seen only if you mirror the packet in the SPB cloud.</p>
wi01136379	<p>A node configured with all supported features and booted with the base license loses all T-UNI configuration.</p> <p>Loading a node with a base license fails to load configuration related to the IP VRF, ISIS, SPBM and IPVPN.</p>	None
wi01137696	<p>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.</p> <p>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.</p>	None

Table continues...

Known issues and limitations

Issue number	Description	Workaround
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
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 <i>not</i> 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 <code>GlobalRouter POE ERROR poeMgrPoeDefaultConfig: POE Driver error (bcm_poe_set_logical_port_map())</code> 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 <code>default SLPP</code> command without parameters, the command does not automatically set all SLPP parameters to default.	Always execute the <code>default SLPP</code> command with appropriate parameters. For example, to set the SLPP parameter <code>tx-interval</code> to default, execute the command <code>default slpp tx-interval</code> .
wi01143509	Redundant RIP configuration is saved for BVLANS when configuration is saved in verbose mode. Sourcing this configuration displays the error <code>RIP circuit for ifindex does not exist</code> .	None
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 <code>default</code> .
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 <code>show spanning-tree rstp port config [{slot/port}[-slot/port][, ...]]</code>	None. This behavior is as designed.

Table continues...

Issue number	Description	Workaround
	displays the value of Port Protocol Migration as <code>false</code> irrespective of whether the protocol migration flag is set to <code>true</code> or <code>false</code> .	
wi01160332	VSP 4450GSX-PWR+ : The command <code>show int gi statistic verbose</code> 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 <code>poe poe-limit <></code> to limit the power to 15.4W if 802.3af standard is configured.
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 <code>sys shutdown</code> 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 <code>shutdown/no-shutdown</code> commands continuously: <pre>IO1 [05/02/14 06:59:55.178:UTC] 0x0011c525 00000000 GlobalRouter COP-SW ERROR vsp4kTxEnable Error changing TX disable for SFP module: 24, code: -8</pre>	None. When this issue occurs, the port in question may go down, then performs a <code>shutdown/no-shutdown</code> of the port to bring it up and resumes operation.
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.

Table continues...

Known issues and limitations

Issue number	Description	Workaround
wi01173136	<p>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.</p>	<p>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.</p>
wi01175118	<p>On a MACsec enabled port, you may see delayed packets when the MACsec port is kept running for more than 12 hours.</p> <p>This delayed packet counter may also increment when there is complete reordering of packets so that the application might receive a slow response.</p> <p>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.</p>	None
wi01175367	<p>The voltage for power supply erroneously displays as 220 volts when the power intake is more than 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.</p>	None
wi01195988	<p>IPv4 Ping/TraceRoute may not work in the EDM.</p>	Use ACLI to initiate ping and traceroute.
wi01196000	<p>Not able to ping or do traceroute to IPv4 address using EDM.</p>	Use ACLI to initiate ping and traceroute.
wi01197547	<p>The output for the show vlan remote-mac-table command can be different than what appears for the same command on VSP 9000.</p> <p>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.</p>	None

Table continues...

Issue number	Description	Workaround
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.
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.
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 <code>show interface gigabitethernet statistics</code> , the OUTLOSS PACKETS counter value increments when packets are dropped as a result of Source Port squelching on NNI ports.	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.	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: <ul style="list-style-type: none"> • 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	Ignore these errors as there are no other ramifications and they do not cause any data loss.

Table continues...

Known issues and limitations

Issue number	Description	Workaround
	clean-up VLAN when the port is already down.	
wi01205572	Spoof-detect may not work when enabled. There are no commands to check the status of a spoof-detect port.	None
wi01205942	LACP MLT: On bouncing both 1G fiber ports on the switch, the second port may not come back up. If we continuously bounce the VSP4850-GTS 1G Fiber port (1/47 or 1/48) using automated scripts in short interval, sometimes it does not come up.	Re-seat the SFP of the respective port.
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.
wi01207711	SPB ethertype 0x8100 is modified to 0x88a8 when packets traverse over Virtual IST.	None
wi01208362	VSPtalk is referenced in "show fulltech". This has no impact on the switch operation.	None
wi01208978	IPv6 UDP packets egressing NNI links go into COS 6 queue.	None
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: <ul style="list-style-type: none"> • 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.
wi01209696	A corner case scenario where an IGMP ACL is applied to block a host from joining	Use ACLs, even if you want to block the only receiver available on the interface.

Table continues...

Issue number	Description	Workaround
	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.	

Limitations in release 4.1

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 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 12: VSP 4450GTX-HT-PWR+ limitations

Issue	Description	Workaround
high-temperature threshold	The VSP 4450GTX-HT-PWR+ supports a temperature range of 0°C to 70°C. The 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.
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.	Ensure that the POE device power draw is maintained at the following when the device is at temperatures between 61°C and 70°C: <ul style="list-style-type: none"> • 400W — with 1 operational power supply • 832W — with 2 operational power supplies

Table 13: 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 Layer 2 VSN. They are dropped by the ingress BEB.

Table continues...

Issue number	Description
	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	<p>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 <code>show ip igmp sender</code> command is not updated with new sender port information.</p> <p>You can perform one of the following workarounds:</p> <ul style="list-style-type: none"> On an IGMP snoop enabled interface, you can flush IGMP sender records. <p> Caution: Flushing sender records can cause a transient traffic loss.</p> <ul style="list-style-type: none"> On an IGMP enabled Layer 3 interface, you can toggle the IGMP state. <p> Caution: Expect traffic loss until IGMP records are built after toggling the IGMP state.</p>
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 Layer 2 VLAN before enabling IGMP snooping on it. After IGMP snooping is enabled on the Layer 2 VLAN for the first time, static multicast group configuration is allowed, even when IGMP snooping is disabled later on that Layer 2 VLAN.
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, <code>4k2:1(config)#isis apply redistribute direct vrf 2</code> .
wi01122478	<p>Stale snmp-server community entries for different VRFs appear after reboot with no VRFs .</p> <p>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 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 .</p>
wi01171670	Telnet packets get encrypted on MACsec enabled ports.
wi01198872	<p>Loss of learned MAC addresses occurs in a vIST setup beyond 10k addresses.</p> <p>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 addresses with a vIST pair, the MAC learning in a vIST setup is limited to 10K Mac addresses.</p>

Chapter 7: Resolved issues in release 4.1

This section details the issues that were resolved in release 4.1.

Table 14: Resolved issues

WI reference	Description
wi01162515	The VSP 4000 switch fails to enable maximum supported ingress (1530) and egress (256) ACEs.
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 a Layer 2 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.
No WI	Physical LEDs for ports 47 and 48 do not light on link up on the switch VSP4450-GSX-PWR+ and VSP4450-GSX.