



Avaya Virtual Services Platform 4000 Release Notes - Release 4.0

Release 4.0
NN46251-401
Issue 04.10
July 2014

© 2014 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 Avaya's computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed, or remotely accessed on hardware products, and any upgrades, updates, 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 Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) 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 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.

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.

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.

Contents

Chapter 1: Introduction	6
Purpose.....	6
Related resources.....	6
Support.....	9
Chapter 2: New in this release	11
Features.....	11
Overview of features and hardware models by release.....	12
Other Changes	18
Chapter 3: Important notices	19
Hardware compatibility.....	19
Platform power supplies.....	20
Supported optical devices	21
Software scaling capabilities.....	25
File names for this release.....	28
Important information and restrictions.....	29
Interoperability notes for VSP 4000 connecting to an ERS 8800.....	29
Supported browsers.....	29
User configurable SSL certificates.....	30
Feature licensing.....	30
Combination ports.....	30
SFP and SFP+ ports.....	31
Shutting down VSP 4000.....	31
Chapter 4: Software Upgrade	34
Image upgrade fundamentals.....	34
Image naming conventions.....	34
Interfaces.....	35
File storage options.....	35
Upgrading the software.....	36
Verifying the upgrade.....	38
Committing an upgrade.....	38
Downgrading the software.....	39
Deleting a software release.....	40
Chapter 5: Supported standards, RFCs, and MIBs	41
Supported IEEE standards.....	41
Supported RFCs.....	42
Quality of service.....	43
Network management.....	43
MIBs.....	44
Standard MIBs.....	45

Proprietary MIBs.....	48
Chapter 6: Known issues and limitations.....	49
Known issues.....	49
Device related issues.....	49
EDM related issues.....	52
Limitations.....	53
Chapter 7: Resolved issues.....	55

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 expected behaviors that may first appear to be issues.

This document does not contain feature updates.

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, you can access the Web site at <http://avaya-learning.com/>.

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to 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

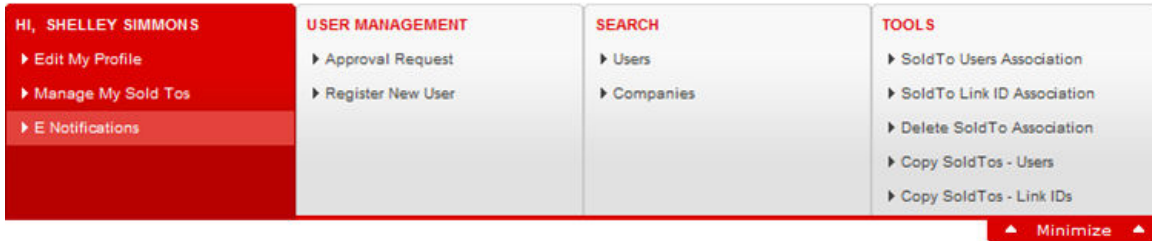
You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Ethernet Routing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

Procedure

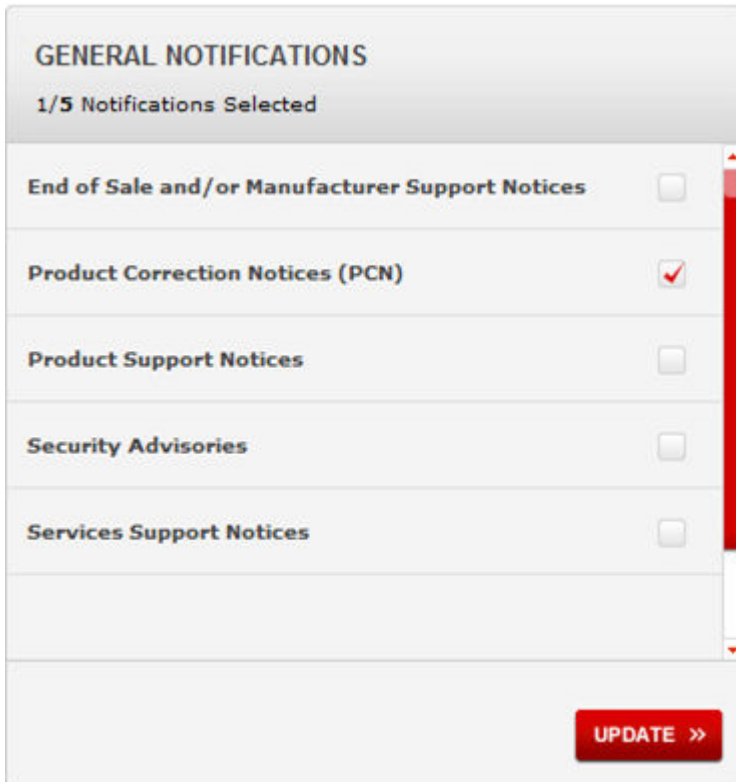
1. In an Internet browser, go to <https://support.avaya.com>.
2. Type your username and password, and then click **LOG IN**.
3. Click **MY PROFILE**.



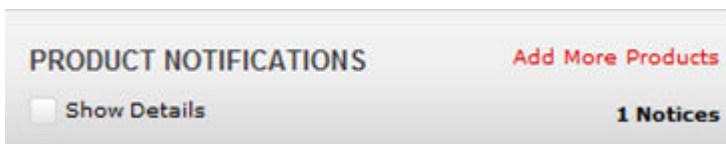
4. On the site toolbar, click your name, and then click **E Notifications**.



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 product names: 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 is titled 'VIRTUAL SERVICES PLATFORM 7000' and features a 'Select a Release Version' dropdown menu set to 'All and Future'. Below this are several checkboxes for documentation categories: Administration and System Programming, Application Developer Information, Application Notes, Application and Technical Notes (checked), Declarations of Conformity, and Documentation Library (checked). A red 'SUBMIT >>' button is located 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 this release

The following sections detail what is new in the *Avaya Virtual Services Platform 4000 Release Notes*, NN46251–401 for Release 4.0.

An overview of software features and hardware models introduced in previous releases up until the current release of the VSP 4000, is also provided.

Related Links

[Features](#) on page 11

[Overview of features and hardware models by release](#) on page 12

[Other Changes](#) on page 18

Features

The following section describes software features and hardware introduced in Release 4.0.

Media Access Control Security (MACsec)

The VSP 4450GSX-PWR+ supports the MACsec feature. MACsec capable LANs provide data origin authenticity, data confidentiality, and data integrity between authenticated hosts/systems. This means the receiver gets the data as-is transmitted by the end host. Every frame exchanged is encrypted and decrypted using the MACsec Key which leads to a secure data communication.

Note:

MACsec feature is supported only on VSP 4450GSX-PWR+. This feature is not supported on the VSP 4850 series models.

For more information, see *Avaya Virtual Services Platform 4000 Series Security*, NN46251–601.

Service Level Agreement Monitor (Avaya diagnostic service)

Virtual Services Platform 4000 Release 4.0 supports the Service Level Agreement Monitor (SLA Mon™) agent as part of the Avaya SLA Mon™ solution.

SLA Mon uses a server and agent relationship to distribute monitoring devices. Use the agent with an SLA Monitor server to perform end-to-end network Quality of Service (QoS) validation, and analyze and monitor the network based on application use and traffic flow. You can use the test results to target under-performing areas of the network for deeper analysis.

For more information, see *Avaya Virtual Services Platform 4000 Series Performance Management*, NN46251–701.

TACACS+

Virtual Services Platform 4000 Release 4.0 supports the TACACS+ client. TACACS+ is a remote authentication protocol that provides centralized validation of users who attempt to gain access to a router or Network Access Server (NAS).

The TACACS+ feature is a client and server-based protocol that allows the VSP 4000 to accept a user name and password and send a query to a TACACS+ authentication server, sometimes called a TACACS+ daemon. The TACACS+ server allows access or denies access, based on the response by the client.

For more information, see *Avaya Virtual Services Platform 4000 Series Security*, NN46251–601.

Equal Cost MultiPath for Virtual routing and forwarding

Virtual Services Platform 4000 Release 4.0 supports Equal Cost MultiPath (ECMP) for Virtual routing and forwarding (VRF).

For more information, see *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505.

New hardware VSP 4450GSX-PWR+

Release 4.0 of Virtual Services Platform 4000 introduces the new hardware chassis 4450GSX-PWR+, with the following features:

- 12 10/100/1000 Base TX RJ-45 ports with 802.3at PoE+
- 36 100/1000 Mbps SFP transceiver modules
- two 1/10G SFP+ ports with MACsec-capable PHY
- one field-replaceable 1000W PSU

For more information, see *Avaya Virtual Services Platform 4000 Series Installation*, NN46251–300.

For more information about hardware models, see [Hardware compatibility](#) on page 19.

SFP+ transceivers

VSP 4000 Release 4.0 introduces support for the following SFP+ transceivers.

Hardware	Description	Part number
10GBASE ZR/ZW SFP+	1550 nm 70km SMF	AA1403016-E6
10GBASE-ER/ZR CWDM (LC)	1471 to 1611 nm with a range up to 70 km	AA1403153-E6 to AA1403168-E6

For more information, see [Supported optical devices](#) on page 21.

Related Links

[New in this release](#) on page 11

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 4.0, 3.1, 3.0.1, and 3.0.

Features for Releases 4.0, 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			
	4.0	3.1	3.0.1	3.0
Operations and Management				
Media Access Control Security (MACSec) on page 11	X			
TACACS+ on page 12	X			
Avaya CLI (ACLI) For more information, see <i>Avaya Virtual Services Platform 4000 Series Command Line Reference Guide</i> , NN46251-104.				X
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 802.1ag Connectivity Fault Management (CFM) For more information, see <i>Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series</i> , NN46251-510.				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 For more information, see <i>Avaya Virtual Services Platform 4000 Series Security</i> , NN46251-601.				X
Secure Shell and Secure Copy Server For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251-600.				X
Secure Shell (SSH) client support				X

Features	New in release			
	4.0	3.1	3.0.1	3.0
For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251–600.				
Simple Loop Prevention Protocol (SLPP) For more information, see <i>Network Design Reference for Avaya Virtual Services Platform 4000 Series</i> , NN46251–200.				X
SLPP Re-Arm For more information, see <i>Network Design Reference for Avaya Virtual Services Platform 4000 Series</i> , NN46251–200.				X
Simple Network Management Protocol (SNMP) For more information, see <i>Avaya Virtual Services Platform 4000 Series Security</i> , NN46251–601.				X
Telnet client and server For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251–600.				X
TFTP Client and Server 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
9k Jumbo packet support For more information, see <i>Avaya Virtual Services Platform 4000 Series Administration</i> , NN46251–600.				X
Layer 2				
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				
IP Multicast over SBPM		X		

Features	New in release			
	4.0	3.1	3.0.1	3.0
For more information, see <i>Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Series</i> , NN46251–510.				
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		
ETree 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 3 IPv4 Routing Services				
Equal Cost MultiPath (ECMP) for Virtual routing and forwarding (VRF) For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – IP Routing</i> , NN46251-505.	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 Global Router (GRT)				X

Features	New in release			
	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.				
IP Static routes For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – IP Routing</i> , NN46251-505.				X
Microsoft NLB ARP multicast-MAC-flooding support For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – IP Routing</i> , NN46251-505.				X
Virtual Router Redundancy Protocol (VRRP) For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – IP Routing</i> , NN46251-505.				X
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 on page 11	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 L2 to L4				X

Features	New in release			
	4.0	3.1	3.0.1	3.0
For more information, see <i>Avaya Virtual Services Platform 4000 Series Configuration – QoS and ACL Based Traffic Filtering</i> , NN46251–502.				
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
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 and 3.x

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

Model	Part number	Release
VSP 4450GSX-PWR+ on page 12	EC4400A04-E6	4.0
VSP 4850GTS	EC4800A78-E6	3.x
	EC4800B78-E6	
	EC4800C78-E6	
	EC4800D78-E6	
	EC4800E78-E6	
	EC4800F78-E6	
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 19, and *Avaya Virtual Services Platform 4000 Series Installation*, NN46251–300.

Related Links

[New in this release](#) on page 11

Other Changes

See the following section for information about changes that are not feature-related.

Software upgrade

This document has been updated with software upgrade information for release 4.0. See [Upgrading the software](#) on page 36.

Software scaling capabilities

This document has been updated with software scaling capabilities information for release 4.0. See [Software scaling capabilities](#) on page 25.

Related Links

[New in this release](#) on page 11

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.

Table 1: Hardware

VSP 4000 model	Description	Part number
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
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	EC4800A88-E6

VSP 4000 model	Description	Part number
	<ul style="list-style-type: none"> one (of two) field replaceable 1000W PSUs supplied with the chassis 	
	<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
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
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 1/10GE SFP+ ports with MACsec capable PHY one (of two) field replaceable 1000W PSUs supplied with the chassis 	EC4400A04-E6

Platform power supplies

The Virtual Services Platform 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 Avaya Virtual Services Platform 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 300W and 1000W 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*
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>		

Supported optical devices

Use optical devices to achieve high bit-rate communications and long transmission distances. The following section describes the supported optical devices on the VSP 4000 system.

Important:

Avaya recommends that you use Avaya branded SFP and SFP+ transceivers as they undergo extensive qualification and testing. Avaya is not responsible for any problems that arise from using non-Avaya branded SFP and SFP+ transceivers.

Small form factor (SFP) pluggable transceivers

SFPs are hot-swappable input and output enhancement components designed to allow gigabit Ethernet ports to link with other gigabit Ethernet ports over various media types.

You can use various SFP (1Gb/s) and SFP+ (10Gb/s) to attain different line rates and reaches. The following table describes the SFPs including the reach provided by various SFPs.

This table is informational only—not all Avaya Ethernet switching and routing products support all the SFPs listed here.

For more information about SFP and SFP+ transceivers, including technical specifications and installation instructions, see *Installing Transceivers and Optical components on the Avaya Virtual Services Platform 4000 Series*, NN46251-301.

! **Important:**

The attainable cable length can vary depending on the quality of the fiber optic cable used.

Table 3: Supported SFP transceivers

Model	ROHS product number	Description
1000BASE-T	AA1419043-E6	CAT5 UTP, up to 100 m. Because the 1000BASE-T device is all electrical, it does not need DDI support.
1000BASE-SX DDI	AA1419048-E6	850 nm up to 275 m using 62.5 m MMF optic cable up to 550 m using 50 µm MMF optic cable
1000BASE-LX DDI	AA1419049-E6	1310 nm, up to 10 km
1000BASE-XD DDI	AA1419050-E6	1310 nm, up to 40 km This transceiver has been discontinued but remains supported by the software.
	AA1419051-E6	1550 nm, up to 40km (non-CWDM) This transceiver has been discontinued but remains supported by the software. Avaya recommends AA1419057-E6 as a replacement.
1000BASE-ZX DDI	AA1419052-E6	1550 nm, up to 70 km (non-CWDM) This transceiver has been discontinued but remains supported by the software. Avaya recommends AA1419065-E6 as a replacement.
1000BASE-BX DDI	AA1419069-E6 and AA1419070-E6 mating pair	One model transmits at 1310 nm and receives at 1490 nm, while the mating model transmits at 1490 nm and receives at 1310 nm. The reach is up to 10km.
	AA1419076-E6 and AA1419077-E6 mating pair	One model transmits at 1310 nm and receives at 1490 nm, while the mating model transmits at 1490 nm and receives at 1310 nm. The reach is up to 40km.
1000BASE-EX DDI	AA1419071-E6	1550 nm, up to 120 km (non-CWDM)
1000BASE DDI CWDM	AA1419053-E6	1470 nm, up to 40 km
	AA1419054-E6	1490 nm, up to 40 km
	AA1419055-E6	1510 nm, up to 40 km
	AA1419056-E6	1530 nm, up to 40 km
	AA1419057-E6	1550 nm, up to 40 km
	AA1419058-E6	1570 nm, up to 40 km

Model	ROHS product number	Description
	AA1419059-E6	1590 nm, up to 40 km
	AA1419060-E6	1610 nm, up to 40 km
	AA1419061-E6	1470 nm, up to 70 km
	AA1419062-E6	1490 nm, up to 70 km
	AA1419063-E6	1510 nm, up to 70 km
	AA1419064-E6	1530 nm, up to 70 km
	AA1419065-E6	1550 nm, up to 70 km
	AA1419066-E6	1570 nm, up to 70 km
	AA1419067-E6	1590 nm, up to 70 km
	AA1419068-E6	1610 nm, up to 70 km
100BASE-FX	AA1419074-E6	1310 nm, up to 2km

Small form factor (SFP+) pluggable plus transceivers

SFP+ transceivers are hot-swappable input and output enhancement components that allow 10 gigabit connections. All Avaya SFP+ transceivers use Lucent connectors (LC) to provide precision keying and low interface losses.

The following table lists and describes the Avaya SFP+ models.

Table 4: Supported SFP+ transceivers and cables

Model number	Part number	Description
10GBASE-CX	AA1403018-E6 to AA1403021-E6	4-pair twinaxial copper cable to connect 10 Gb ports. The maximum range is 15 m.
10GBASE-ER/EW	AA1403013-E6	1550 nm SMF. The range is up to 40 km.
10GBASE-ER CWDM DDI	AA1403153-E6	1471 nm SMF. The range is up to 40 km.
	AA1403154-E6	1491 nm SMF. The range is up to 40 km.
	AA1403155-E6	1511 nm SMF. The range is up to 40 km.
	AA1403156-E6	1531 nm SMF. The range is up to 40 km.
	AA1403157-E6	1551 nm SMF. The range is up to 40 km.
	AA1403158-E6	1571 nm SMF. The range is up to 40 km.
	AA1403159-E6	1591 nm SMF. The range is up to 40 km.

Model number	Part number	Description
	AA1403160-E6	1611 nm SMF. The range is up to 40 km.
10GBASE-LR/LW	AA1403011-E6	1310 nm SMF. The range is up to 10 km.
10GBASE-LRM	AA1403017-E6	1310 nm. Up to 220 m reach over Fiber Distributed Data Interface (FDDI)-grade 62.5 µm multimode fiber. Suited for campus LANs.
10GBASE-SR/SW	AA1403015-E6	850 nanometers (nm). The range is up to the following: <ul style="list-style-type: none"> • 26 m using 62.5 micrometer (µm), 160 megaHertz times km (MHz-km) MMF • 33 m using 62.5 µm, 200 MHz-km MMF • 66 m using 62.5 µm, 400 MHz-km MMF • 82 m using 50 µm, 500 MHz-km MMF • 300 m using 50 µm, 2000 MHz-km MMF • 400 m using 50 µm, 4700 MHz-km MMF (OM4)
10GBASE-ZR/ZW	AA1403016-E6	1550 nm SMF. The range is up to 70 km.
10GBASE-ZR CWDM DDI	AA1403161-E6	1471 nm SMF. The range is up to 70 km.
	AA1403162-E6	1491 nm SMF. The range is up to 70 km.
	AA1403163-E6	1511 nm SMF. The range is up to 70 km.
	AA1403164-E6	1531 nm SMF. The range is up to 70 km.
	AA1403165-E6	1551 nm SMF. The range is up to 70 km.
	AA1403166-E6	1571 nm SMF. The range is up to 70 km.
	AA1403167-E6	1591 nm SMF. The range is up to 70 km.
	AA1403168-E6	1611 nm SMF. The range is up to 70 km.


Optical power considerations

When you connect the device to collocated equipment, ensure that enough optical attenuation exists to avoid overloading the receivers of each device. You must consider the minimum attenuation requirement based on the specifications of third-party equipment. For more information about minimum insertion losses for Avaya optical products, see *Installing Transceivers and Optical components on the Avaya Virtual Services Platform 4000 Series*, NN46251-301.


Software scaling capabilities

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


Table 5: Software scaling capabilities

	Maximum number supported
Layer 2	
IEEE/Port-based VLANs	4059
LACP	24 aggregators
LACP ports per aggregator	8 active and 8 standby
MACs in forwarding database (FDB)	32,000
Multi-Link Trunking (MLT)	24 groups
Multiple Spanning Tree Protocol (MSTP)	12 instances
Protocol-based VLANs	1
Rapid Spanning Tree Protocol (RSTP)	1 instance
SLPP	128 VLANs
VLACP Interfaces	50
Layer 3	
RIP interfaces	24
RIP routes	500
OSPF interfaces	48 (24 of these can be passive)
OSPF adjacencies	24
OSPF areas (per system)	64
OSPF routes per VRF	16,000  Note: The maximum routes supported per VRF is 16000. The 16000 routes can be distributed across the 24 VRFs (+ GRT) in any manner. If all 24 VRFs are operational, 640 routes per VRF are supported.

Important notices

	Maximum number supported
OSPF routes	16,000
OSPF VRF support	24
e-BGP peers	12
e-BGP routes	16,000
Address Resolution Protocol (ARP) for each port, VRF, or VLAN (IPv4)	6,000 entries total
Circuitless IP interfaces	64
Maximum B-MACs	1000
ECMP routes	1000
ECMP groups	<p>512 groups with a maximum of 4 ECMP paths per group</p> <p> Note:</p> <p>The maximum number of ECMP routes per VSP 4000 system is 1000.</p> <p>So, for example, if 500 ECMP groups are configured, the maximum number of ECMP paths per group is 2 and if 250 ECMP groups are configured, the maximum number of ECMP paths per group is 4.</p>
ECMP paths per route	4
FIB IPv4 routes	16,000
RIB IPv4 routes	16,000
IPv4 interfaces	256
Maximum VRFs	24
IPv4 CLIP interfaces	64
IP routing policies	500 for each VRF 5,000 for each system
IPv4 FTP sessions	4
IPv4 Rlogin sessions	8
IPv4 SSH sessions	8
IPv4 Telnet sessions	8
IPv4 VRF instances	24
Static ARP entries (IPv4)	200 for each VRF 1,000 for each system
Static routes (IPv4)	1,000 per VRF/per system
UDP/DHCP forwarding entries	128 for each system
VRRP interfaces (IPv4)	64

	Maximum number supported
VRRP interfaces fast timers (200 ms)	24
Diagnostics	
Mirrored ports	49
Remote Mirroring Termination (RMT) ports	4
Filters and QoS	
Port shapers (IPv4)	50
Access control lists (ACL) for each switch	Ingress: 256 Egress: 126
ACEs for each ACL or switch	Ingress: 766 Egress: 252
SPBM	
C-VLANs per VSP 4000 node	1000
Maximum number of nodes per region	1000
MAC entries	16,000 (combination of ARP entries and Layer 2 MACs)
Backbone MAC	1,000
IP routes in the Global Router	16,000
Maximum IS-IS IP routes	16,000
IS-IS interfaces	24
IS-IS adjacencies per VSP 4000 node	24
Layer 2 VSN ISIDs per VSP 4000 node	1,000
Layer 3 VSN ISIDs per VSP 4000 node	24
IP Multicast over SPB	
Maximum unique IGMP group records per node	1000
Maximum unique Multicast Streams (S,G,V) sourced per node	1000
Maximum number of Multicast ISIDs (VSP 4000 acting as a BEB and/or BCB)	32,000
Maximum number of Layer 2 VSNs with Multicast enabled	1000
Maximum number of Layer 3 VSNs with Multicast enabled	24
Maximum number of IP interfaces with Multicast enabled	256
Number of remote senders that can be received on each VSP 4000 node, for the Universal Plug and Play Group (239.255.255.250)	3500

	Maximum number supported
Maximum unique multicast streams sourced per VSP 4000 node	1000
T-UNI	
T-UNI ISIDs per VSP 4000 node	48
Maximum MAC limit on a T-Uni I-SID	32,000
 Note: This is also the device limit.	

File names for this release

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 6: 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.4.0.0.0.tgz	173,311,756
Encryption Module	Encryption module for Avaya Virtual Services Platform 4000 Series.	VSP4K.4.0.0.0_modules.tgz	79,467

Table 7: 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.	VSP4000v400_HELP_EDM_gzip.zip	2,644,709

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 8: Open Source software files

File name	Description	Size
VSP4K.4.0.0.0_oss-notice.html	Master copyright file. This file is located in the Licenses directory.	414,245
VSP4K.4.0.0.0_OpenSource.zip	Open source base software for Virtual Services Platform 4000 Release 4.0.	95,850,520

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**.

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/4.0.0.0.GA/release/oss-notice.txt`.

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 26

User configurable SSL certificates

Virtual Services Platform 4000 does not generate SSL certificates with user-configurable parameters. You can, however, use your own certificate.

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

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

If you use a Base license, you do not need to install a license file. If you purchase an Advanced or Premier license, you must obtain and install a license file. For more information about how to generate and install a license file, see *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600.

Important:

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

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

Combination ports

When the VSP 4000 is reset, the peer connections for all ports, including combination ports 47 and 48 on VSP 4850GTS and VSP 4850GTS-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

- SFP and SFP+ ports support 1000Base-T SFP (RJ-45) for 1000Mbps. Triple-speed mode is not supported.
- SFP+ port does not support slow speed SFPs. Supports 10G and 1G.

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-4850GTS:1>enable
```

```
VSP-4850GTS: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
```

```
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
```

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.

Related Links

[Image naming conventions](#) on page 34

[Interfaces](#) on page 35

[File storage options](#) on page 35

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

Related Links

[Image upgrade fundamentals](#) on page 34

Interfaces

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

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

Related Links

[Image upgrade fundamentals](#) on page 34

File storage options

This section details what you must know about the internal boot and system flash memory, Universal Serial Bus (USB) mass-storage device, and external flash, which you can use to store the files that start and operate the Virtual Services Platform 4000.

The Virtual Services Platform 4000 file system uses long file names.

Internal flash

The Virtual Services Platform 4000 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 Virtual Services Platform 4000, or to download the software to the internal flash memory, external flash, or USB device.

The Virtual Services Platform 4000 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 external flash.

Related Links

[Image upgrade fundamentals](#) on page 34

Upgrading the software

Perform this procedure to upgrade the software on the Avaya VSP 4850 GTX PWR+. This procedure shows how to upgrade the software using the internal flash memory as the file storage location.

 **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 40.

Supported upgrade paths on the VSP 4850 GTX PWR+:

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

Before you begin

- Back up the configuration files.
- Use an FTP application to 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-4850GTS-PWR+:1>enable
```

```
VSP-4850GTS-PWR+:1#configure terminal
```

```
VSP-4850GTS-PWR+:1(config)#boot config flag ftpd
```

```
VSP-4850GTS-PWR+:1>exit
```

```
VSP-4850GTS-PWR+:1#software add VSP4K.4.0.0.0.tgz
```

```
VSP-4850GTS-PWR+:1# software add-modules 4.0.0.0.GA VSP4K.4.0.0.0_modules.tgz
```

```
VSP-4850GTS-PWR+:1#software activate 4.0.0.0.GA
```

```
VSP-4850GTS-PWR+:1#reset

VSP-4850GTS-PWR+:1#show software
=====
                        software releases in /intflash/release/
=====
VSP4K.4.0.0.0int064 (Backup Release)
4.0.0.0.GA (Primary Release)
-----
Auto Commit      : enabled
Commit Timeout   : 10 minutes

VSP-4850GTS-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 36.

Procedure

1. Enter Privileged EXEC configuration mode:

```
enable
```

2. Remove software:

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

Example

```
VSP-4850GTS-PWR+:1>enable
```

```
VSP-4850GTS-PWR+:1#software remove VSP4K.4.0.0.0.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 9: 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-2004	Port-Based Network Access Control
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
802.3i	10BaseT
802.3u	100BaseT

IEEE standard	Description
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 10: Supported request for comments

Request for comment	Description
draft-grant-tacacs-02.txt	TACACS+ Protocol
RFC768	UDP Protocol
RFC783	Trivial File Transfer Protocol (TFTP)
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	FTP and TFTP client and server
RFC1027	Using ARP to implement transparent subnet gateways/Nortel Subnet-based VLAN
RFC1122	Requirements for Internet Hosts
RFC1256	ICMP Router Discovery
RFC1305	Network Time Protocol v3 Specification, Implementation and Analysis
RFC1340	Assigned Numbers
RFC1519	Classless Interdomain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC1541	Dynamic Host Configuration Protocol1
RFC1542	Clarifications and Extensions for the Bootstrap Protocol

Request for comment	Description
RFC1591	DNS Client
RFC1812	Router requirements
RFC1866	Hypertext Markup Language version 2 (HTMLv2) protocol
RFC2068	Hypertext Transfer Protocol
RFC2131	Dynamic Host Control Protocol (DHCP)
RFC2138	RADIUS Authentication
RFC2139	RADIUS Accounting
RFC2338	Virtual Redundancy Router Protocol (VRRP)
RFC2616	Hypertext Transfer Protocol 1.1
RFC2819	Remote Network Monitoring (RMON)
RFC2992	Analysis of an Equal-Cost Multipath Algorithm
RFC3046	DHCP Option 82
RFC3621	PoE – Power over Ethernet
RFC4250–RFC4256	SSH server and client support
RFC6329	IS-IS Extensions supporting Shortest Path Bridging

Quality of service

Table 11: Supported request for comments

Request for comment	Description
RFC2474 and RFC2475	DiffServ Support
RFC2597	Assured Forwarding PHB Group
RFC2598	An Expedited Forwarding PHB

Network management

Table 12: Supported request for comments

Request for comment	Description
RFC1155	SMI
RFC1157	SNMP
RFC1215	Convention for defining traps for use with the SNMP

Request for comment	Description
RFC1271	Remote Network Monitoring Management Information Base
RFC1305	Network Time Protocol v3 Specification, Implementation and Analysis
RFC1350	TFTP (Revision 2)
RFC1354	IP Forwarding Table MIB
RFC1757	Remote Network Monitoring Management Information Base
RFC1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1908	Coexistence between v1 and v2 of the Internet-standard Network Management Framework
RFC1930	Guidelines for creation, selection, and registration of an Autonomous System (AS)
RFC2541	Secure Shell Protocol Architecture
RFC2571	An Architecture for Describing SNMP Management Frameworks
RFC2572	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC2573	SNMP Applications
RFC2574	User-based Security Model (USM) for v3 of the Simple Network Management Protocol (SNMPv3)
RFC2575	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC2576	Coexistence between v1, v2, and v3 of the Internet standard Network Management Framework
RFC2819	Remote Network Monitoring Management Information Base

MIBs

Table 13: Supported request for comments

Request for comment	Description
RFC1156	MIB for network management of TCP/IP
RFC1212	Concise MIB definitions
RFC1213	TCP/IP Management Information Base
RFC1354	IP Forwarding Table MIB

Request for comment	Description
RFC1389	RIPv2 MIB Extensions
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)
RFC1573	Interface MIB
RFC1650	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC1657	BGP-4 MIB using SMIv2
RFC1850	OSPF MIB
RFC2096	IP Forwarding Table MIB
RFC2578	Structure of Management Information v2 (SMIv2)
RFC2674	Bridges with Traffic MIB
RFC2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC2863	Interface Group MIB
RFC2925	Remote Ping, Traceroute & Lookup Operations MIB
RFC3416	v2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC4113	Management Information Base for the User Datagram Protocol (UDP)

Standard MIBs

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

Table 14: Supported MIBs

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
STDMIB2— Link Aggregation Control Protocol (LACP) (802.3ad)	802.3ad	ieee802-lag.mib


Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
STDMIB4—Internet Assigned Numbers Authority (IANA) Interface Type	—	iana_if_type.mib
STDMIB5—Structure of Management Information (SMI)	RFC1155	rfc1155.mib
STDMIB6—Simple Network Management Protocol (SNMP)	RFC1157	rfc1157.mib
STDMIB7—MIB for network management of Transfer Control Protocol/Internet Protocol (TCP/IP)-based Internet MIB2	RFC1213	rfc1213.mib
STDMIB8—A convention for defining traps for use with SNMP	RFC1215	rfc1215.mib
STDMIB10—Definitions of Managed Objects for Bridges	RFC1493	rfc1493.mib
STDMIB11—Evolution of the Interface Groups for MIB2	RFC2863	rfc2863.mib
STDMIB12—Definitions of Managed Objects for the Ethernet-like Interface Types	RFC1643	rfc1643.mib
STDMIB15—Remote Network Monitoring (RMON)	RFC2819	rfc2819.mib
STDMIB17—Management Information Base of the Simple Network Management Protocol version 2 (SNMPv2)	RFC1907	rfc1907.mib
STDMIB21—Interfaces Group MIB using SMIv2	RFC2233	rfc2233.mib
STDMIB26a—An Architecture for Describing SNMP Management Frameworks	RFC2571	rfc2571.mib
STDMIB26b—Message Processing and Dispatching for the SNMP	RFC2572	rfc2572.mib
STDMIB26c—SNMP Applications	RFC2573	rfc2573.mib
STDMIB26d—User-based Security Model (USM) for version 3 of the SNMP	RFC2574	rfc2574.mib
STDMIB26e—View-based Access Control Model (VACM) for the SNMP	RFC2575	rfc2575.mib

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
STDMIB26f —Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework	RFC2576	rfc2576.mib
STDMIB29—Definitions of Managed Objects for the Virtual Router Redundancy Protocol	RFC2787	rfc2787.mib
STDMIB31—Textual Conventions for Internet Network Addresses	RFC2851	rfc2851.mib
STDMIB32—The Interface Group MIB	RFC2863	rfc2863.mib
STDMIB33—Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations	RFC2925	rfc2925.mib
STDMIB38—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
STDMIB39—Entity Sensor Management Information Base	RFC3433	
STDMIB40—The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model	RFC3826	rfc3826.mib
STDMIB41—Management Information Base for the Transmission Control Protocol (TCP)	RFC4022	rfc4022.mib
STDMIB43—Management Information Base for the User Datagram Protocol (UDP)	RFC4113	rfc4113.mib
STDMIB44—Entity MIB	RFC4133	rfc4133.mib
STDMIB45—Definitions of Managed Power over Ethernet	RFC3621	rfc3621.mib
STDMIB??—SecY Management Table (secylfTable)	802.1ae	8021ae.mib

Proprietary MIBs

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

Table 15: Proprietary MIBs

Proprietary MIB name	File name
PROMIB1—Rapid City MIB  Note: The MACsec tables, namely, rcMACSecCAtable and rcMACSecIfConfigTable are a part of the Rapid City MIB.	rapid_city.mib
PROMIB 2—SynOptics Root MIB	synro.mib
PROMIB3—Other SynOptics definitions	s5114roo.mib
PROMIB4—Other SynOptics definitions	s5tcs112.mib
PROMIB5—Other SynOptics definitions	s5emt103.mib
PROMIB6—Avaya RSTP/MSTP proprietary MIBs	nnrst000.mib, nnmst000.mib
PROMIB11—Avaya MIB definitions	wf_com.mib
PROMIB12—Other SynOptic definition for Combo Ports	s5ifx.mib
PROMIB31—Other SynOptic definition for PoE	bayStackPethExt.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

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

Device related issues

Table 16: 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
wi01114420	<p>When a route is redistributed into ISIS, you may see the following warning message: SW WARNING ISIS local rmap head is null, using global. This message provides additional information for the development team and does not indicate</p>	None.

Known issues and limitations

Issue number	Description	Workaround
	any operational errors; it can be safely ignored.	
wi01126761	Traffic convergence can take 3 to 6 seconds for NNI failover on a BEB with a large number (greater than 600) of L2 VSNs.	None.
wi01134509	On a T-UNI port, with incoming untagged traffic, the internal QoS level of the traffic flow is set to 0, irrespective of the L2 Trust configuration on the port. If incoming client packets are untagged, the internal priority queue of the VSP 4000 is always the best-effort queue.	None.
wi01136168	The <code>metric</code> field in the <code>redistribute</code> command is not supported for inter-VRF redistributed routes. This impacts only inter-VRF metric settings. It does not impact inter-VRF route filtering.	None.
wi01137696	A port or a VLAN based filter created for CFM, OSPF, RIP, PIM, or VRRP control protocols with a Deny/Permit action (ACE or Global-ctrl-pkt action), based on ethertype/ip/other qualifiers, bypasses the filter rules. A port based filter created on T-UNI port or MLT for LACP, VLACP control protocols with a Deny/Permit action (ACE or Global-ctrl-pkt action), based on ethertype/ip/other qualifiers, bypasses the filter rules.	None.
wi01137736	On a base VSP 4000 system with Revision 10 hardware and POE support, PAUSE frames are not supported.	None.
wi01138070	The 802.1 priority bits in the BVLAN tag are not copied to the I-Tag when traffic egresses out of the NNI port.	None.
wi01140395	Pinging a remote IP address over VRF does not work unless the source IP address is specified.	None.
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.

Issue number	Description	Workaround
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> .
wi01144867	On the port that is removed from a T-UNI LACP MLT, non T-UNI configuration is blocked as a result of T-UNI consistency checks.	When a port is removed from a T-UNI LACP MLT, the LACP key of the port must be set to default.
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: 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	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.
wi01170924	VSP 4850GTS: On running the command <code>no-shutdown</code> , the following invalid configuration warning message appears on the logging screen: COP-SW WARNING cb_sw_port_set_speed warning: bcm_port_speed_set: unit 0 port 52 speed 10 : Invalid configuration	None. Occurs only in a corner case scenario with Combo ports (1/47,1/48) & only in GTS box, port speed is set correctly so no functional impact.
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.

Issue number	Description	Workaround
wi01173026	A reboot with verbose configuration does not allow you to delete any vrf.	This issue occurs only when the configuration file is saved in "verbose" mode and then rebooted in that configuration. On field, it is highly unlikely to save a configuration file in verbose mode and use that for sourcing the configuration. Verbose mode is used more as a diagnostic tool. This issue does not impact the functionality of the product.
wi01173136	T1 SFP: Shutting down the T1 link from one end of the VSP 4000 does not shut down the link at the remote end. You may experience traffic loss if the remote side of the link is not shut down.	This issue occurs only when T1 SFP link from one end is shutdown. Enable a dynamic link layer protocol such as LACP or VLAC on both ends to shut the remote end down too. As an alternative, administratively disable both the ends of the T1 SFP link to avoid the impact.
wi01175118	On a MACsec enabled port, you may see delayed packets when the MACsec port is kept running for more than 12 hours. This delayed packet counter may also increment when there is complete reordering of packets so that the application might receive a slow response. But in this case, it is a marginal increase in the packet count, that occurs due to PN mismatch sometimes only during Key expiry, and does not induce any latency.	None.
wi01175367	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.	None.

EDM related issues

Table 17: Known issues

Issue number	Description	Workaround
wi01096275	The EDM tab IS-IS > Stats > IS-IS > Interface Counters and Tab > Stats > Interface Control Packet shows the circuit index for each entry instead of the interface	The circuit index and interface mapping is instead displayed in the EDM tab IS-IS > IS-IS > Interface . Use this tab to find the interface for the circuit index.

Issue number	Description	Workaround
	index. From this tab, you cannot tell what interface the IS-IS circuit is using.	
wi01132300	In the EDM, the output of the T-UNI ISID FDB entries when filtered on a port that is part of an MLT is not consistent with the ACLI output.	In the EDM, enter the corresponding MLT ID instead of the port.

Limitations

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.

Table 18: Limitations and expected behaviors

Issue number	Description
wi01159075	VSP 4450GSX-PWR+ : Mirroring functionality is not working for RSTP BPDUs
wi01145099	IP multicast packets with TTL=1 are not switched across the SPB cloud over an L2 VSN. They are dropped by the ingress BEB. To prevent IP multicast packets from being dropped, configure multicast senders to send traffic with TTL >1.
wi01138851	Configuring and Retrieving licenses using the EDM is not supported.
wi01112491	IS-IS enabled ports cannot be added to an MLT. The current release does not support this configuration.
wi01142142	When a multicast sender moves from one port to another within the same BEB, with the old port operationally up, the source port information in the output of the <code>show ip igmp sender</code> command is not updated with new sender port information. You can perform one of the following workarounds: <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> On an IGMP enabled L3 interface, you can toggle the IGMP state. <p>⚠ Caution: Expect traffic loss until IGMP records are built after toggling the IGMP state.</p>
wi01143223	Hosts connected to a VSP 4000 system acting as a VRRP backup-master, cannot ping the VRRP virtual IP, if the VRRP session is established over an L2-VSN between the VRRP master and backup-master for that VLAN. However, traffic from

Issue number	Description
	the hosts is routed by the VRRP backup-master, and the ARP for the VRRP virtual IP is resolved.
wi01141638	When a VLAN with 1000 multicast senders is deleted, the console or telnet session hangs and SNMP requests time out for up to 2 minutes.
wi01137195	A static multicast group cannot be configured on an L2 VLAN before enabling IGMP snooping on it. After IGMP snooping is enabled on the L2 VLAN for the first time, static multicast group configuration is allowed, even when IGMP snooping is disabled later on that L2 VLAN.
wi01068569	The system displays a warning message that routes will not inject until the apply command is issued after the enable command. The warning applies only after you enable redistribution, and not after you disable redistribution. For example, <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>
wi01136327	In Ingress BEB, CVLAN priority bits are reversed if the incoming customer packet is driven out of queue 0 or 1. Original CVLAN priority is restored in Egress BEB.
wi01171670	Telnet packets get encrypted on MACsec enabled ports.
wi01135628	<p>Remarking of dot1p for tagged unicast, unknown unicast, or multicast traffic fails on L2 trusted T-UNI ports. This issue is not seen on CVLAN ports.</p> <p>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.</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>
wi01138595	The OUTLOSS PACKETS counter value increments when packets are dropped, as a result of Source Port squelching on T-UNI ports.

Chapter 7: Resolved issues

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

Table 19: Resolved issues

WI reference	Description
Device related issues	
wi01142727	For traffic coming from an SPBM cloud and egressing VSP 4000 towards a UNI port, all client frames have the 802.1 priority bits set to zero, if the ingress BEB is a VSP 9000 system.
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>
wi01166823	VSP 4450GSX-PWR+: The MCoSPB sender traffic does not egress out of NNI Receiver port of the system when the CPU is hiked consistently. Avoiding CPU hikes over longer periods of time solves the issue.
wi01163425	VSP 4000: Executing the command <code>show ip route</code> causes a crash if the remote IS-IS system host name is configured with the maximum permitted length.
wi01163084	The Association Number is incorrect in the message logged for key refresh.
wi01161534	VSP 4450GSX-PWR+ (PoE): The 802.3af standard allows 21W of power to PD. The workaround was to limit the power to 15.4W if 802.3af standard is configured. This is no longer necessary.
wi01160531	VSP 4450GSX-PWR+ : When routes are increased to more than 16,000, the system crashes and a Core Dump is generated. The maximum number of supported routes in the system is 16,000. This is as per design. The system crashes only when this limit is crossed.
wi01155740	VSP 4450GSX-PWR+ : The output of the ACLI command <code>show poe-port-status</code> shows "DeliveringPower" when connected to a non-PoE 4850GTS system and "OtherFault" when connected to PoE 4850GTS system.
wi01092747	An abort from a FTP client session may not be processed right away, but may be delayed for up to 60 seconds. During this time the FTP session may show as active.
wi01094114	The CLI <code>copy</code> command may in some cases not return an error if the remote FTP or TFTP server cannot accept the file due to a full disk. The file may be created with a file size of zero.

Resolved issues

WI reference	Description
wi01096785	The ARP aging timer is broken.
wi01098428	On an Etree setup, after isis is reset, the mac entries are not learned.
wi01078025	On import, filter ACL default action as deny with control-packet-action as permit is not working. When filter ACL default action is configured as deny and control-packet-action is permit, control packets are dropped by the filter default action.
wi01091986	On one occasion a core dump has been detected following the <code>reset</code> command as the system was shutting down; the reboot sequence completed successfully and the switch came back online.
wi01093170	The show clock does not display the updated time-zone value.
wi01093913	The one shot <code>snmpset</code> command does not work for the creation and isid set for an Etree Private VLAN.
wi01094391	Configuration of BVLAN with vlan id 1, under router isis should not be allowed.
wi01094393	Unable to provide the burst-count value with the <code>loopback</code> command when the <code>interframe-interval</code> option is used.
wi01094840	The following message appears when the switch is booting: <code>WARNING: Check dummy: modes fastethernet_interface_configurationspanning-tree.</code>
wi01095494	QoS Code clean up and functionality on a 10G port when in 1G mode should have the same functions that the 1G ports use.
wi01096198	When a MAC-in-MAC packet is encapsulated at the SPB edge, the packet priority is carried into the pbits in the BTAG and the pbits in the ITAG, and both priority values should be consistent. However, sometimes the priority in the ITAG is not marked correctly, so that the ITAG may carry the priority
wi01096838	Disable L3VSN Mac learning.
wi01098490	The license logging event ID 0x000000658 is shared with/by the internal error code log.
wi01098746	Port the fix that resolved the <code>nnlinnclip</code> segmentation fault.
wi01099822	If you assign a Vlan name that is longer than the display field for the commands <code>show vlan basic</code> , and <code>show vlan advance</code> , then the alignment of <code>show vlan advance</code> is improper in the output.
wi01100726	Cannot disable <code>ip routing</code> on a VRF
wi01101004	Support for <code>control-packet-action</code> of the ACL default action in ACLI is required.
wi01103000	The debug config file should not be overwritten.
wi01103789	The L3 VSN router is not learnt when there are 256 IP interfaces; and is not learnt dynamically if you delete 2 IP addresses. The workaround is to disable and then enable the router isis.
wi01104529	Customer ARP and ICMP request packets with VLAN priority 0 received on a UNI interface are being transmitted out the NNI interface with BVLAN priority equal to 6.

WI reference	Description
wi01105101	GlobalRouter ISIS ERROR plsbScProcessBmac:getPortFromMgid Failed:Dest:00bb.0000.6500.00 VlanId:4001 mgid 229 port 1/38.
wi01105277	The system displays the wrong error when you change <code>encap dot1q</code> for <code>lacp mlt</code> .
wi01106504	Remove command <code>slot shutdown</code> because there is no Out-Of-Band Mgmt port.
wi01108234	The system displays the following error after boot: 0x0031c605 00000000 GlobalRouter POE ERROR poeMgrPoeDefaultConfig: POE Driver error (bcm_poe_set_logical_port_map() error: -4).
wi01108248	Requires port fix for SPB crash.
wi01108477	The <code>flight-recorder archive</code> command logs SW Error Process died messages.
wi01108927	SNMP MIB walk stack dumps switch.
wi01108939	SNMP failure on <code>isis TimeStamp</code> definition.
wi01110177	EDM: changing the <code>encap dot1q</code> for an <code>lacp</code> interface fails with unknown error.
wi01110188	The <code>copy clilog</code> command executes with errors referring to the VSP 9000 platform.
wi01110194	Enabling edge port on an MLT interface fails with the error <code>operation not allowed</code> , and with the console and log message <code>GlobalRouter HW INFO Admin Edge Port status changes will take effect only after the port is bounced</code> .
wi01110914	The command <code>sysDescr</code> does not return the correct format which causes COM to not identify the device.
wi01111182	The brouter port <code>vlan</code> should not be allowed to be configured as the <code>ACL inVlan</code> .
wi01111396	Mirrored traffic seen on an private MLT port, from a filter created to permit , count, and mirror all <code>pvlan</code> traffic to a destination <code>mlt</code> , is never removed even after the filter is deleted.
wi01111398	Mirroring a port to a destination MLT fails. If the port to which the mirrored traffic is hashed, then the port is shut down.
wi01112536	The switch crashes when you delete ISIS SPBM configuration through COM 3.0.2 from EDM 3.0.1.
wi01086954	When <code>isis</code> is enabled on a port which is member of <code>vlan 1</code> , the port is not removed from <code>vlan 1</code> automatically. Since <code>isis</code> adds the <code>nni</code> ports to <code>BVLAN</code> automatically when the <code>isis</code> is enabled, the ports are not removed from <code>vlan 1</code> . If the <code>nni</code> port is member of <code>vlan 1</code> , it could possibly trigger <code>mac flush</code> in the <code>cvlans</code> when the <code>nni</code> port state changes.
wi01095069	When IP ECMP is enabled on the <code>i-sid</code> enabled VRF, L3 VSN traffic which hashes out on secondary <code>BVID</code> will be dropped. The root cause is because IP ECMP enabled is not supported on the <code>I-SID</code> VRF on this release. There is no

WI reference	Description
	consistency check in place to not allow the ECMP to be enabled while the VRF is configured the L3 VSP service.
wi01097860	Auxiliary 2 Monitoring should not be implemented for SFP/SFP+ in the <code>show pluggables</code> command.
wi01098477	EDM ISIS > ISIS > Adjacency & EDM ISIS > ISIS > Protocol Summary is not lining up with ACLI.
wi01103444	The default ISIS system ID in <code>config</code> does not load after boot.
wi01112181	The <code>rc.0</code> file can cause continuous crash and reboot if the command in <code>rc.0</code> is not a VSP 4000 known command.
wi01094633	The command <code>clear mlt</code> must be removed from CLI.
wi01127897	If the member ports of the MLT have MSTP disabled and one of the members is removed from the MLT, then all the ports in the original MLT configuration go into an MSTP-enabled state and MSTP reconverges.
wi01134468	On a T-UNI port with L2 untrusted configuration, the internal QoS of the traffic flow is derived from the .1p bits of the ingress tagged traffic. If incoming client packets are tagged, the VSP 4000 system always derives the internal priority queue from the 802.1p tag.
wi01153937	VSP 4450GSX-PWR+ : An FX100 inserted into a port on a GSX device fails to link to another GSX device.
wi01156330	VSP 4450GSX-PWR+ : A working 1G SFP that is connected in 10G slot does not receive any traffic even if the SFP is detected and the link state is 'operation up'.
wi01156384	VSP 4450GSX-PWR+ : The RPS LED appears in OFF state after adding a second power supply without power.
wi01157220	VSP 4450GSX-PWR+ : The error message <code>HW ERROR SEEPROM reading failed on slot PS 1</code> appears when you insert a redundant power supply with power.
wi01157967	VSP 4450GSX-PWR+ : The interval between the first two NTP messages is 15 minutes although NTP interval is set to 10 minutes.
wi01158219	ECMP : The VSP 4000 system crashes when ECMP is enabled or disabled with ECMP static route having the prefix-list mapped to pathlist-2.
wi01158854	VSP 4450GSX-PWR+ : The Rx Port counter statistics on ports 1/49 and 1/50 display double the number of packets than that transmitted from SMB.
wi01159615	A one-time crash is seen when you try to execute IGMP commands.
wi01159915	VSP 4450GSX-PWR+ : ISIS adjacency does not converge when <code>shutdown</code> and <code>no shutdown</code> commands are run on NNI ports when the system is initially brought up.
wi01161022	VSP 4450GSX-PWR+ : If the PoE limit is set to less than the PoE load on a port, the port status changes to "OtherFault" and does not change even after changing the PoE limit to a higher value.
wi01161587	VSP 4450GSX-PWR+ (10G ports): The state of the 10G link is 'up' in CP, but the state is 'down' in BCM even though the remote end state is 'admin down'.

WI reference	Description
wi01161728	VSP 4450GSX-PWR+ : The 10G port drops all packets whose size is above 1559 bytes.
wi01162463	The system crashes on running <code>show ip arp</code> command after running <code>shutdown</code> and <code>no shutdown</code> commands on NNI link on the box with 2K ARP entry.
wi01166373	VSP 4450GSX : The LACP link does not come up on failover, when 10G ports are configured as LACP MLT.
wi01168172	VSP 4000 : With copper and fiber Ethernet ports as part of NNI LACP MLT, all traffic ingressing from UNI gets duplicated on the NNI, when traffic is hashed on to the fiber NNI links.
wi01169291	VSP4000 Release 4.0 Trials : The optic with part number AA1419075-E6 shows as unsupported on the VSP 4000 system.
wi01170771	The system crashes when you execute the command <code>show interfaces gigabitEthernet <port-id-range></code> .
wi01172580	Core-dump occurs when a host route with a next-hop of itself pointing to another VRF is deleted. Fix is in file <code>/vob/nd_protocols/rtn/lib/rtnbase.cpp</code> . Check for the next-hop pointer before accessing the file.
EDM related issues	
wi01163338	VSP 4450GSX-PWR+ : The EDM does not show the SFP/DDI tab for ports 1/13 to 1/48.
wi01163331	VSP 4000: The Device Physical view on the EDM does not indicate whether an SFP or SFP+ is installed or not.
wi01096060	EDM fails the port stat refresh when table items are selected and the bar graph is selected with cumulative results.
wi01096082	EDM fails stat refresh when 15 or more ports are selected.
wi01096089	EDM fails stat refresh for cumulative results when you clear the results.
wi01159075	In EDM, the VRF ip route table interface information is not displayed for route entry.
wi01101458	The range for Vlan aging time must be changed from 0...1000000 to 0.
wi01103729	When you have private vlans, and then create a new mlt and refresh EDM to view the updated vlan list, EDM experiences an endless loop and eventually times out.
wi01105461	There is inconsistent behavior when you create a vlan of type protocol ipv6 using ACLI and EDM.
wi01107796	If you launch EDM through COM, the ARP table for the VRF window does not populate with any entries.
wi01109986	If you launch EDM through COM, the Vlan FDB aging time does not allow you to configure on VRF, and does not display timer information.
wi01110515	If you open a 6th EDM session, the system closes an existing EDM session before opening a new session.
wi01110811	In EDM, the ip route VRF table displays the wrong interface id.

Resolved issues

WI reference	Description
wi01113271	If you launch EDM through COM, the ip route VRF table displays the wrong interface id.
wi01103336	In EDM, the cp-limit tab must be removed from MLT because cp-limit support has been removed in VSP 4000.
wi01155830	VSP 4450GSX-PWR+ : In the EDM, the USB tab in Edit > Filesystem and Edit > Card windows does not correctly display the files on the USB drive.
wi01157917	VSP4K-GSX : In EDM, the 1/50 port displays the incorrect RSTP values (oper p2p, oper version).
wi01169608	VSP 4000 : The Digital Diagnostic Interface displays voltage in milli-volts instead of volts.