Release Notes - Release 3.0.1.0
Avaya Virtual Services Platform 4000

Release 3.0.1.0
NN46251-401
Issue 02.02
November 2013

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 generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by 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 its hardware and Software (“Product(s)”). 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. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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. “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.

Licence types

Designated System(s) License (DS). End User may install and use each copy 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, 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”. 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, or hardware provided by Avaya. All content on this site, the documentation 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 that 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”). 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. 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. 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 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 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, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document describes important information about this first 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.

Related resources

Related topics:

Documentation on page 7
Training on page 7
Avaya Mentor videos on page 8

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/.

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to http://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 site.

Subscribing to e-notifications

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

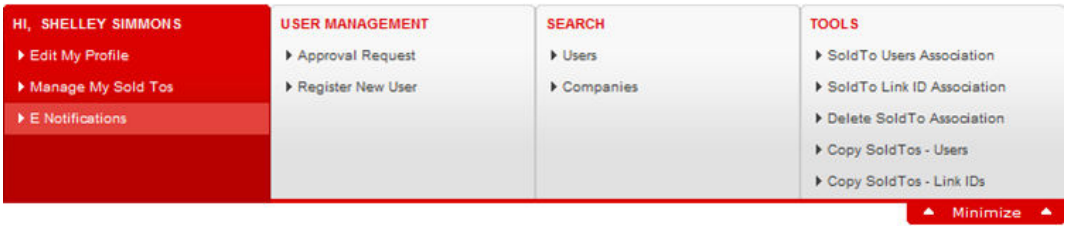
About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), that 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.

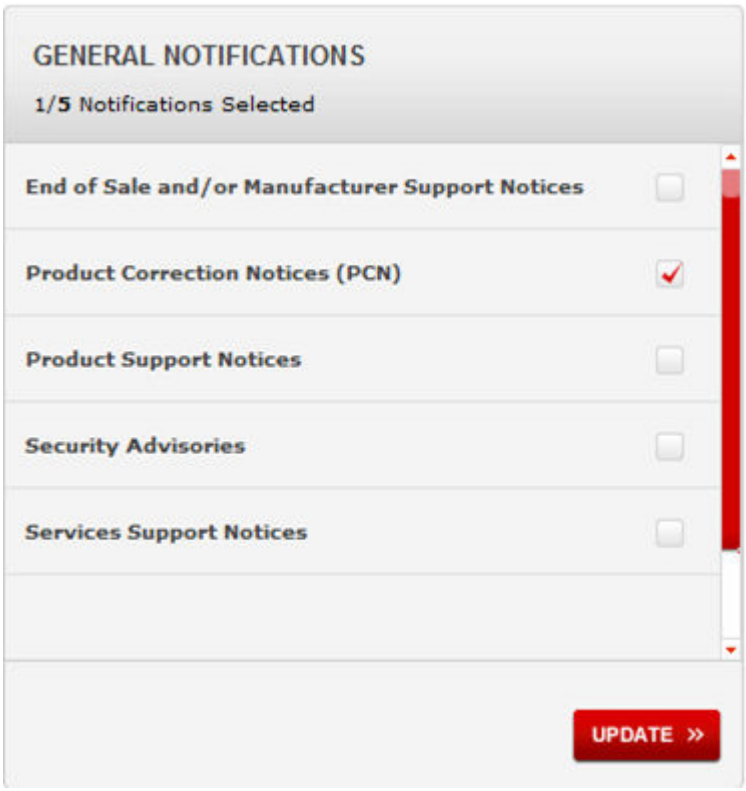
Procedure

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**.

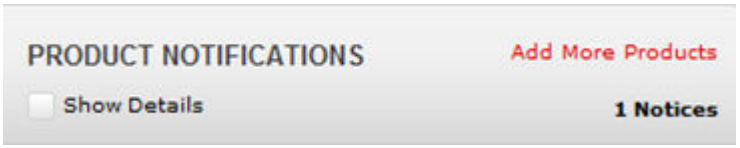
4. On the site toolbar, click your name, and then select **E Notifications**.



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

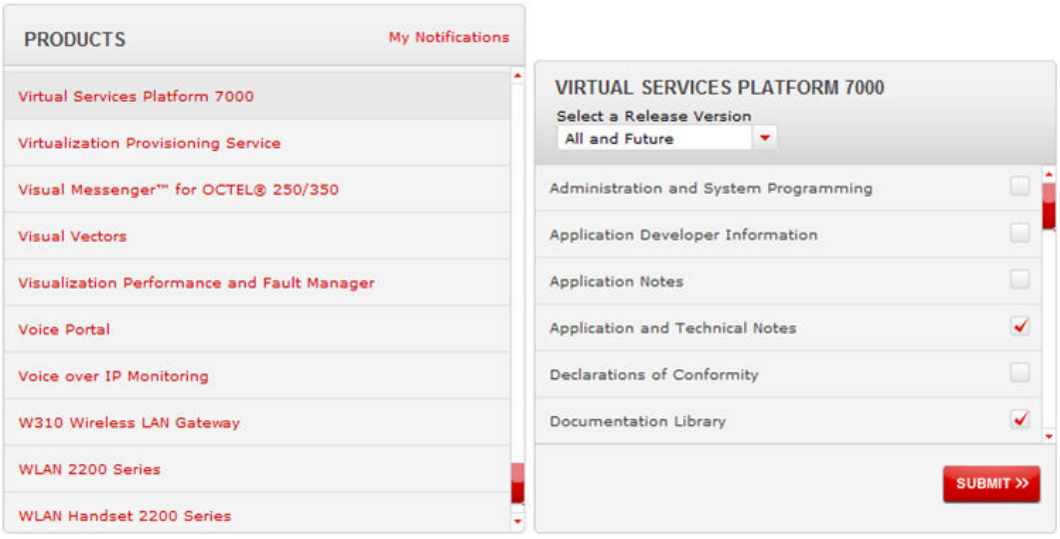


6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.



8. Scroll through the list, and then select the product name.
9. Select a release version.

10. Select the check box next to the required documentation types.



11. Click **Submit**.

Support

Visit 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.

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 3.0.1.0.

Features

Private VLAN

Private VLANs provide isolation between ports within a Layer 2 service.

For more information about private VLANs, see *Avaya Virtual Services Platform 4000 Configuration — VLANs and Spanning Tree*, NN46251-500.

ETree configuration

Private VLANs consist of a primary and secondary VLAN. Etree allows the private VLANs to traverse a SPBM network by associating a private VLAN with an I-SID.

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

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 hardware.

Table 1: Hardware

VSP 4000 model	Description	Part number
VSP 4850GTS	• 48 10/100/1000 BaseTX RJ-45 ports • two SFP ports • two SFP+ ports • Base Software License • one field replaceable 300W PSU	EC4800A78-E6
	• Same content as EC4800A78-E6 with a EU power cord.	EC4800B78-E6
	• Same content as EC4800A78-E6 with a UK power cord.	EC4800C78-E6
	• Same content as EC4800A78-E6 with a JP power cord.	EC4800D78-E6
	• Same content as EC4800A78-E6 with a NA power cord.	EC4800E78-E6
	• Same content as EC4800A78-E6 with a EU power cord.	EC4800F78-E6
VSP 4850GTS-PWR+	• 48 10/100/1000 802.3at PoE+ • two SFP ports • two SFP+ ports	EC4800A88-E6

VSP 4000 model	Description	Part number
	• Base Software License • one field replaceable 1000W PSU	
	• Same content as EC4800A88-E6 with a EU power cord.	EC4800B88-E6
	• Same content as EC4800A88-E6 with a UK power cord.	EC4800C88-E6
	• Same content as EC4800A88-E6 with a JP power cord.	EC4800D88-E6
	• Same content as EC4800A88-E6 with a NA power cord.	EC4800E88-E6
	• Same content a EC4800A88-E6 with a AU power cord.	EC4800F88-E6
VSP 4850GTS DC	• 48 10/100/1000 Base TX RJ-45 ports • two shared SFP ports • two 10GE SFP+ ports • one field replaceable 300W DC PSU	EC4800078-E6
Redundant power supplies		
300W AC redundant power supply	For use in the ERS 4626GTS, 4850GTS, VSP 4850GTS and WL8180, WL8180-16L wireless controllers. [EUED RoHS 5/6 compliant].	AL1905?08-E5*
Stackable 1000W AC POE + power supply.	For use in 4X00 PWR+,	AL1905?21-E6*
Redundant 300W DC power supply.	For use in the VSP 4850GTS-DC, ERS5698TFD, 5650TD, and 5632FD. (EUED RoHS 5/6 compliant). DC connector included	AL1905005-E5
*__Note__: The seventh character (?) of the switch order number must be replaced with the proper letter to indicate desired product nationalization. See the following for details: “A”: No power cord included. “B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden. “C”: Includes power cord commonly used in the United Kingdom and Ireland. “D”: Includes power cord commonly used in Japan. “E”: Includes North American power cord. “F”: Includes Australian power cord.		

Table 2: Compatible SFPs and SFP+s

For more information about SFP and SFP+, see *Avaya Virtual Services Platform 4000 Installation — SFP and SPF+ transceivers* (NN46251–301).

Hardware	Description	Part number
10GBASE-LR/LW SFP+	1310 nm SMF with a range up to 10 km	AA1403011-E6
10GBASE-ER/EW SFP+	1550 nm SMF with a range up to 40 km	AA1403013-E6
10GBASE-SR/SW SFP+	850nm with a range up to 300 m	AA1403015-E6
10GBASE-LRM SFP+	220 m, 1260 to 1355 nm; 1310 nm nominal MMF	AA1403017-E6
10GBase-CX	4-pair twinaxial copper cable that plugs into the SFP+ socket and connects two 10 Gb ports. The maximum range is 10m.	AA1403018-E6
10GBase-CX	4-pair twinaxial copper cable that plugs into the SFP+ socket and connects two 10 Gb ports. The maximum range is 3m.	AA1403019-E6
10GBase-CX	4-pair twinaxial copper cable that plugs into the SFP+ socket and connects two 10 Gb ports. The maximum range is 5m.	AA1403020-E6
1000BASE-T (RJ-45) SFP	Gigabit Ethernet, RJ-45 connector	AA1419043-E6
1000BASE-SX (LC) DDI	850 nm, Gigabit Ethernet, duplex LC connector	AA1419048-E6
1000BASE-LX (LC) DDI	1310 nm, Gigabit Ethernet, duplex LC connector	AA1419049-E6
1000BASE-XD DDI	1310 nm, Gigabit Ethernet, duplex LC connector	AA1419050-E6
	1550 nm, Gigabit Ethernet, duplex LC connector	AA1419051-E6
1000BASE-ZX DDI	1550 nm, Gigabit Ethernet, duplex LC connector	AA1419052-E6
1000BASE-ZX CWDM (LC)	1470 nm to 1610 nm, up to 70 km	AA1419061-E6 to AA1419068-E6
1000BASE-BX bidirectional SFP	1310 nm, single fiber LC, up to 10 km	AA1419069-E6
1000BASE-BX bidirectional SFP	1490 nm, single fiber LC, up to 10 km	AA1419070-E6
1000BASE-EX DDI SFP	1550 nm, up to 120 km	AA1419071-E6

Hardware	Description	Part number
1000BASE-BX bidirectional SFP	1310 nm, single fiber LC, up to 40 km	AA1419076–E6
1000BASE-BX bidirectional SFP	1490 nm, single fiber LC, up to 40 km	AA1419077–E6
100BASE-FX SFP	1310 nm, LC connector	AA1419074-E6

Important:

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

Software scaling capabilities

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

Table 3: Software scaling capabilities

	Maximum number supported
Layer 2	
IEEE/Port-based VLANs	4000 for demo/1000 practical
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

	Maximum number supported
OSPF areas (per instance/per system)	64
OSFP routes per VRF	100 (2400 local OSPF routes in 24 VRFs)
OSPF routes	16,000
OSPF VRF support	4
e-BGP peers	12
e-BGP routes	16,000
Address Resolution Protocol (ARP) for each port, VRF, or VLAN	6,000 entries total
Circuitless IP interfaces	64
ECMP routes	1024
ECMP paths per route	8
FIB IPv4 routes	16,000
IPv4 interfaces	256
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	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
VRRP interfaces fast timers (200 ms)	24
Diagnostics	
Mirrored ports	49
Remote Mirroring Termination (RMT) ports	4
Filters and QoS	
Port shapers (IPv4)	50
ACEs per ACL (a combination of Security and QoS ACEs)	1,000

	Maximum number supported
Unique redirect next hop values for ACE Actions (IPv4)	Ingress: 1,536, Egress: 256
SPBM	
MAC entries	16,000 (combination of ARP entries and Layer 2 MACs)
Backbone MAC	1,000
IP routes in the Global Router	25,000
IS-IS IP routes	16,000
IS-IS adjacencies	24
Layer 2 VSNs	1,000
Layer 3 VSNs	24

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 4: Software Build 64 components

Module or File Type	Description	File Name	File Size (bytes)
Standard Runtime Software Image	Standard image for the Avaya Ethernet Routing Switch 4000 Series	VSP4K.3.0.0.0.tgz	75,234,072
Enterprise Device Manager Help Files	Help files required for Avaya Ethernet Routing Switch 4000	VSP4000v300_HELP_EDM_gzip.zip	2,097,393

Table 5: Software files

File name	Description	Size (bytes)
VSP4K.3.0.0.0_modules.tgz	Encryption modules	37,795

Open Source software files

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

Table 6: Open Source software files

File name	Description	Size
VSP4K.3.0.0.0_oss-notice.html	Master copyright file. This file is located in the Licenses directory.	412 KB
VSP4K.3.0.0.0_OpenSource.zip		96 MB

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/3.0.0.0.GA/release/oss-notice.txt`.

Upgrading the software

Perform this procedure to upgrade the software on the Avaya Virtual Services Platform 4000. 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 21.

Supported upgrade paths:

Upgrade path	Support
Upgrade 3.0.0 to 3.1.0	Supported

Upgrade path	Support
Upgrade 3.0.1 to 3.1.0	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 3.1.0.0, 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:
   ```
   enable
   ```
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>enable

VSP-4850GTS-PWR+:1#software add VSP4K.3.1.0.0.tgz

VSP-4850GTS-PWR+:1# software add-modules 3.1.0.0.GA
VSP4K.3.0.1.0_modules.tgz

VSP-4850GTS-PWR+:1#software activate 3.1.0.0.GA

VSP-4850GTS-PWR+:1#reset

VSP-4850GTS-PWR+:1#show software
================================================================================
                    software releases in /intflash/release/
================================================================================
VSP4K.3.1.0.0int064 (Backup Release)
3.1.0.0.GA (Primary Release)

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

VSP-4850GTS-PWR+:1#software commit
```

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 19.

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.3.0.1.0.tgz
```

Important information and restrictions

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

Interoperability notes for VSP 4000 connecting to an ERS 8800

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

Supported browsers

Virtual Services Platform 4000 supports the following browsers to access the Enterprise Device Manager (EDM):

- Microsoft Internet Explorer 8.0
- Mozilla Firefox 7.x

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 *Avaya Virtual Services Platform 4000 Administration*, 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 *Avaya Virtual Services Platform 4000 Administration*, 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, 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.

Chapter 4: 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 supports.

Supported IEEE standards

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

Table 7: Supported IEEE standards

IEEE standard	Description
802.1aq	Shortest Path Bridging (SPB)
802.1AX	Link Aggregation Control Protocol (LACP)
802.1p	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	Extended Authentication Protocol (EAP), and EAP over LAN (EAPoL)
802.1X-2004	Port Based Network Access Control
802.3 CSMA/CD Ethernet ISO/IEC 8802	International Organization for Standardization (ISO) /International Eletrotechnical Commission (IEC) 8802-3
802.3ab	Gigabit Ethernet 1000BaseT 4 pair Category 5 (Cat5) Unshieled Twisted Pair (UTP)
802.3ae	10 Gigabit Ethernet
802.3af and 802.3at	PoE – Power Over Ethernet
802.3i	10BaseT

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

Supported RFCs

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

Table 8: Supported request for comments

Request for comment	Description
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

Request for comment	Description
RFC1519	Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC1541	Dynamic Host Configuration Protocol1
RFC1542	Clarifications and Extensions for the Bootstrap Protocol
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	VRRP: Virtual Redundancy Router Protocol
RFC2616	Hypertext Transfer Protocol 1.1
RFC2819	RMON
RFC2992	Analysis of an Equal-Cost Multi-Path 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 9: 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 10: Supported request for comments

Request for comment	Description
RFC1155	SMI
RFC1157	SNMP
RFC1215	Convention for defining traps for use with the SNMP
RFC1271	Remote Network Monitoring Management Information Base
RFC1305	Network Time Protocol v3 Specification, Implementation and Analysis3
RFC1350	The TFTP Protocol (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 & 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)

Request for comment	Description
RFC2576	Coexistence between v1, v2, & v3 of the Internet standard Network Management Framework
RFC2819	Remote Network Monitoring Management Information Base

MIBs

Table 11: 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
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

Request for comment	Description
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 supports.

Table 12: 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
STDMIB3—Exensible Authentication Protocol Over Local Area Networks (EAPoL) (802.1x)	802.1x	ieee8021x.mib
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	RFC1213	rfc1213.mib

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
Protocol (TCP/IP) based Internet MIB2		
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
STDMIB26f —Coexistence between Version 1, Version	RFC2576	rfc2576.mib

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
2, and Version 3 of the Internet-standard Network Management Framework		
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

Proprietary MIBs

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

Table 13: Proprietary MIBs

Proprietary MIB name	File name
PROMIB1 – 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 5: 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 14: Known issues

Issue number	Description	Workaround
wi01111785	Internal QoS remapping with filters is not working for certain UDP destination ports. This is due to the control packets in the VSP 4000 system that are assigned with higher priority egress queue. The action to assign the incoming control packet with egress queue is in conflict with the action of the egress queue derived from the internal QoS remapping with ACL filter. Hence, the internal QoS remapping with ACL filter does not work for those control packets.	The control packets received from the ingress port include the following: • Always assign queue-6: DHCP, BPDU, LLDP, SLPP, CFM, ARP, IST-ARP1, IST-SLM, BARP, EAP, PIM-MC, PIM-UC, RIPv2, RIPv1, OSPF-MC, OSPF-UC, IGMP, BGP, TELNET, SSH, RSH, RLOGIN, TFTP, FTP, RADIUS, NTP, ICMP, HTTP, HTTPS, IPV6-ND. • Always assign queue-7: ISIS control, LACP, VLACP, VRRP, SNMP, IST
wi01114420	When a route is redistributed into ISIS, you may see the following warning message: `SW WARNING ISIS`	None.

Issue number	Description	Workaround
	`local rmap head is null, using global.` This message provides additional information for the development team and does not indicate any operational errors, and may be safely ignored.	

EDM related issues

Table 15: Known issues

Issue number	Description	Workaround
wi01096275	The EDM tab **IS-IS** > **Stats** > **IS-IS** > **Interface Counters and Tab** > **Stats** > **Interface Control Packet** show the circuit index for each entry instead of the interface index. From this tab, you cannot tell what interface the ISIS circuit is using.	The circuit index and interface mapping is shown in EDM tab **IS-IS** > **IS-IS** > **Interface**. Go to this tab to find the interface for the circuit index.
wi01112398	If we launch EDM through COM, CFM-l2 ping does not work, and displays a timeout error. EDM plug-in may not display the **Result** field of the tab of **Edit** > **Diagnostics** > **L2Ping/L2Traceroute** > **L2Ping** properly if the field contains a special character such as "new line" or "tab". This field is a read-only field.	Use on-box EDM or CLI to run the CFM-l2 ping and traceroute testing.

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 16: Limitations and expected behaviors

Issue number	Description
wi01068569	The system displays a warning message that routes will not inject until the apply command is issued after the enable command. The warning applies only after you enable redistribution, and not after you disable redistribution. For example, `4k2:1(config)#isis apply redistribute direct vrf 2`.
wi01122478	Stale snmp-server community entries for different VRFs appear after reboot with no VRFs . On an node with any valid config file saved with more than the default vrf0 , snmp_community entries for that VRF are created and maintained in a separate txt file, snmp_comm.txt, on every boot. The node reads this file and updates the snmp 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 .
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.
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.
wi01136327	On a T-Uni port, the .1p bit of the CVLAN in the egress packet is changed when the .1p bits of the ingress tagged traffic is 0 or 1.

Chapter 6: Resolved issues

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

Table 17: Resolved issues

WI reference	Description
Device related issues	
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 `copy` 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.
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 `reset` 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 `snmpset` 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 `loopback` command when the `interframe-interval` option is used.
wi01094840	The following message appears when the switch is booting: `WARNING: Check dummy: modes fastethernet_interface_configurationspanning-tree`.
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

WI reference	Description
	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 nnclinnclip segmentation fault.
wi01099822	If you assign a Vlan name that is longer than the display field for the commands `show vlan basic`, and `show vlan advance`, then the alignment of `show vlan advance` is improper in the output.
wi01100726	Cannot disable `ip routing` on a VRF
wi01101004	Support for `control-packet-action` 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.
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 `encap dot1q` for `lacp mlt`.
wi01106504	Remove command `slot shutdown` 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 `flight-recorder archive` command logs SW Error Process died messages.
wi01108927	SNMP MIB walk stack dumps switch.
wi01108939	SNMP failure on isis `TimeStamp definition`.
wi01110177	EDM: changing the `encap dot1q` for an `lacp` interface fails with unknown error.

WI reference	Description
wi01110188	The `copy clilog` command executes with errors referring to the VSP 9000 platform.
wi01110194	Enabling edge port on an MLT interface fails with the error `operation not allowed`, and with the console and log message `GlobalRouter HW INFO Admin Edge Port status changes will take effect only after the port is bounced`.
wi01110914	The command `sysDescr` does not return the correct format which causes COM to not identify the device.
wi01111182	The brouter port vlan should not be allowed to be configured as the ACL inVlan.
wi01111396	Mirrored traffic seen on an private MLT port, from a filter created to permit , count, and mirror all pvlan traffic to a destination mlt, 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 isis is enabled on a port which is member of vlan 1, the port is not removed from vlan 1 automatically. Since isis adds the nni ports to BVLAN automatically when the isis is enabled, the ports are not removed from vlan 1. If the nni port is member of vlan 1, it could possibly trigger mac flush in the cvlans when the nni port state changes.
wi01095069	When IP ECMP is enabled on the i-sid enabled VRF, L3 VSN traffic which hashes out on secondary BVID will be dropped. The root cause is because IP ECMP enabled is not supported on the I-SID VRF on this release. There is no 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 `show pluggables` command.
wi01098477	**EDM ISIS** > **ISIS** > **Adjacency & EDM ISIS** > **ISIS** > **Protocol Summary** is not lining up with ACLI.
wi01103444	The default ISIS system ID in `config` does not load after boot.
wi01112181	The rc.0 file can cause continuous crash and reboot if the command in rc.0 is not a VSP 4000 known command.
wi01094633	The command `clear mlt` must be removed from CLI.
EDM related issues	
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.

WI reference	Description
wi01096089	EDM fails stat refresh for cumulative results when you clear the results.
wi01098835	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.
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.