Release Notes for Avaya Virtual Services Platform 9000

Release 4.0.1
NN46250-401
Issue 08.01
July 2015

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

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

Licence types

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

Heritage Nortel Software

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

Copyright

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose

This document describes new features and important information about the latest release. Release notes include a list of known issues (including workarounds where appropriate) and a list of resolved issues. This document also describes known limitations and expected behaviors that may first appear to be issues.

Related resources

Documentation

See *Documentation Reference for Avaya Virtual Services Platform 9000,* NN46250-100 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 website at http://avaya-learning.com/.

Course code	Course title
4D00010E	Knowledge Access: ACIS - Avaya ERS 8000 and VSP 9000 Implementation
5D00040E	Knowledge Access: ACSS - Avaya VSP 9000 Support

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Subscribing to e-notifications

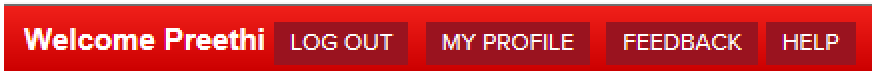
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

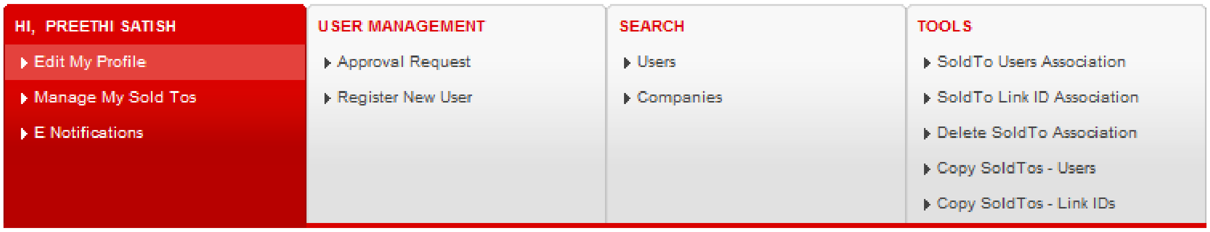
You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Ethernet Routing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

Procedure

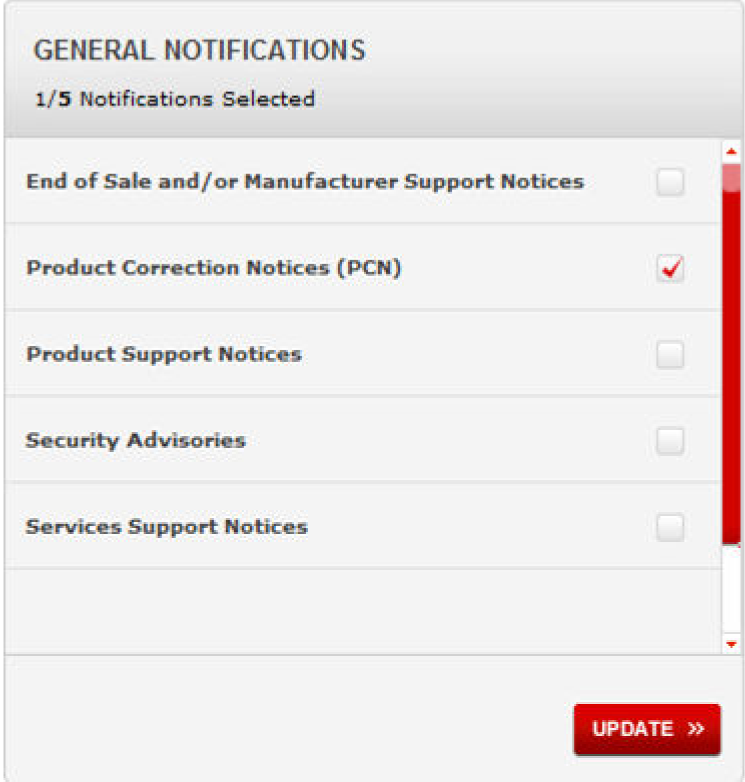
1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Click **MY PROFILE**.



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



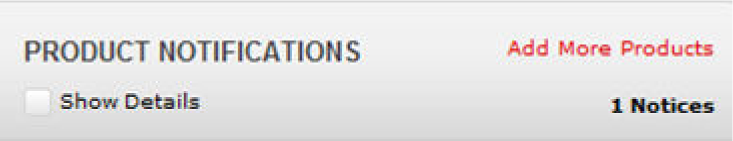
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.


GENERAL NOTIFICATIONS

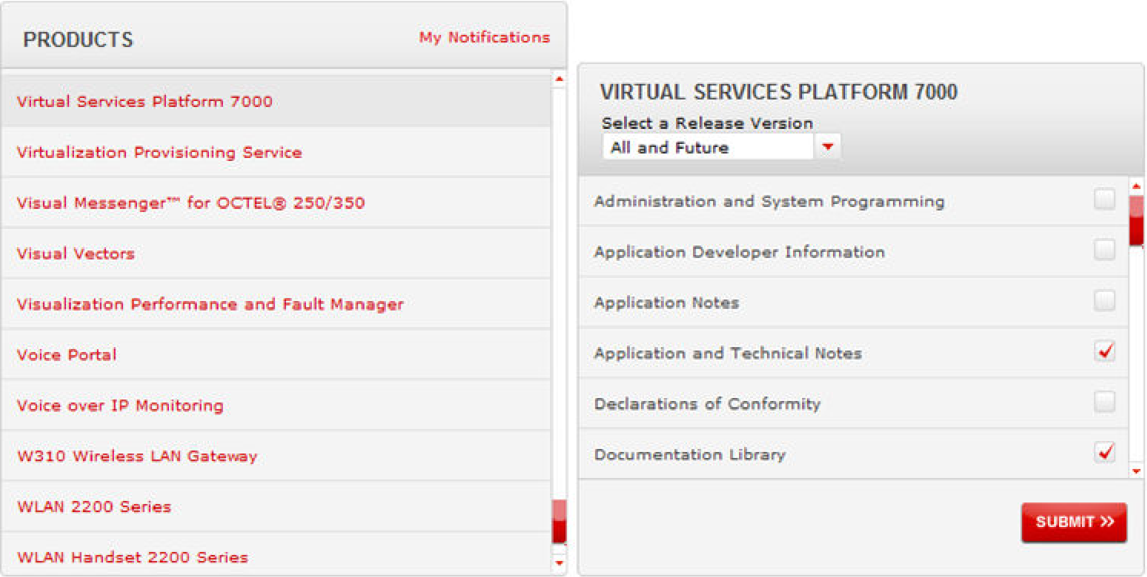
1/5 Notifications Selected

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

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



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



PRODUCTS

My Notifications

- 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
- WLAN Handset 2200 Series

VIRTUAL SERVICES PLATFORM 7000

Select a Release Version: All and Future

- Administration and System Programming □
- Application Developer Information □
- Application Notes □
- Application and Technical Notes ☑
- Declarations of Conformity □
- Documentation Library ☑

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 describe what is new in *Release Notes for Avaya Virtual Services Platform 9000,* NN46250-401 for Release 4.0 and 4.0.1.

Features in Release 4.0.1

New hardware support

Release 4.0.1 adds support for the following new hardware:

- 9012QQ-2 Input/Output (I/O) module
- 40GBASE-LR4 QSFP+ (AA1404001-E6)
- 40GBASE-SR4 QSFP+ (AA1404005-E6)
- QSFP+ to QSFP+ 40-gigabit, 0.5, 1, 3, and 5 meter Direct Attach Cable (DAC) assemblies, which directly connect two QSFP+ ports.

For more information about new hardware, see the following sections:

- New hardware supported on page 17
- Hardware scaling capabilities on page 32

IPv6 routing

❗ **Important:**

Do not upgrade to Release 4.0.1 if you have IPv6 configuration. IPv6 configuration is deleted and cannot be restored.

Support for IPv6 routing is temporarily disabled in Release 4.0.1 for all I/O modules. Support for IPv6 routing will be restored in a future release and all references to IPv6 remain in the documentation.

Features in Release 4.0

See the following sections for information about feature changes.

IPv6 routing

Important:

Do not upgrade to Release 4.0 if you have IPv6 configuration. IPv6 configuration is deleted and cannot be restored.

Support for IPv6 routing is temporarily disabled in Release 4.0 for all I/O modules. Support for IPv6 routing will be restored in a future release and all references to IPv6 remain in the documentation.

IPFIX

IPFIX has been modified in Release 4.0 for use by second generation I/O modules. These modifications include:

- Flow export
- IPFIX templates
- IPFIX sampling

IPFIX recorded flows for second generation I/O modules can no longer be monitored on the system directly. An external collector and monitor must be used.

See Chapter 5 in *Monitoring Performance on Avaya Virtual Services Platform 9000,* NN46250-701 for information on the configuration and use of IPFIX.

New feature support

Release 4.0 adds the following new software features:

- Second generation mode.
- Scaling enhancements for IPv4 FIB routes.
- Scaling enhancements for Intermediate-System-to-Intermediate (IS-IS) adjacencies.
- IS-IS accept policies with Layer 3 VSNs or IP Shortcuts.

For more information about new software features, see New features on page 16 and Software and hardware scaling capabilities on page 32.

New hardware support

Release 4.0 adds support for the following new hardware:

- 9048XS-2 Input/Output (I/O) module.
- 10GBase–LR SFP+ (AA1403011-E6HT)
- 10GBase–SR SFP+ (AA1403015-E6HT)

For more information about new hardware, see the following sections:

- New hardware supported on page 17
- Hardware scaling capabilities on page 32

9012FCHS

The 9012FCHS high-speed cooling module is added to the documentation. Use the 9012FCHS high-speed cooling module for the Virtual Services Platform 9012 to support second generation I/O modules. See *Installing Cooling Modules in Avaya Virtual Services Platform 9000,* NN46250-302 for more information.

Features and hardware by release

Features and hardware models by release on page 69 is added to this document to track feature introduction.

Shutting down a VSP 9000 system

Shutting down the system on page 28 is added. The functionality is not new to Release 4.0 but the procedure is new to the document.

Unsupported command

Beginning with Release 4.0, the **`boot config loadconfigtime`** command is no longer supported.

Other changes

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

Document title change

In Release 4.0, the title of this document changed from *Avaya Virtual Services Platform 9000 Release Notes*, NN46250–401 to *Release Notes for Avaya Virtual Services Platform 9000,* NN46250-401.

Chapter 3: Important notices and new features

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

Table 1: Important Notices

COM 3.1.1 will introduce support for Virtual Services Platform 9000 Release 4.0.
Virtual Services Platform 9000 second generation I/O modules do not support Lossless Ethernet using ACLI or EDM for Release 4.0..
Virtual Services Platform 9000 does not support IPv6 configuration using ACLI or EDM for Release 4.0. ❗ **Important:** Save your configuration file if it contains IPv6 information. The IPv6 configuration is removed once you upgrade to Release 4.0.

Installing new I/O modules

Use this procedure to install the 9048XS-2 or 9012QQ-2 I/O module.

Before you begin

When installing the I/O module, ensure you have:

- Release 4.0.1 software.
- 9048XS-2 or 9012QQ-2 I/O module.
- 9012FCHS modules if using the Virtual Services Platform 9012 chassis.
- The required number of Switch Fabrics.

  ❗ **Important:**

  A minimum of five Switch Fabrics are required to run the I/O module, however six are needed if redundancy is required.

Procedure

1. Upgrade the software to Release 4.0.1.0 following the upgrade steps in *Applying Upgrades and Patches to Avaya Virtual Services Platform 9000* (NN46250-400).

2. Confirm that all services are working as expected.

Next steps

Before inserting the module:

1. When using the Virtual Services Platform 9012 chassis, replace both cooling modules with 9012FCHS modules.

   Important:

   Replacing only one cooling module in the Virtual Services Platform 9012 chassis will result in the module being non-operational.

   Important:

   If using the 9010 chassis no change of the cooling modules is required.

2. Insert additional Switch Fabric modules as needed.

   Important:

   A minimum of five Switch Fabrics are required to run the I/O module, however six are needed if redundancy is required.

3. Insert the I/O module into the chassis.

4. Ensure the status LED turns green and all ports light up.

5. The following is an example of the log messages displayed with a successful installation:

   ```
   CP1  [09/21/14 10:13:20.082] 0x00010750 00000000 GlobalRouter HW INFO Module
   9048XS-2 in slot 10 is ready for configuration download
   CP1  [09/21/14 10:13:20.083] 0x00010758 00000000 GlobalRouter HW INFO Downloading
   configuration to all cards
   CP1  [09/21/14 10:13:20.085] 0x00088512 00000000 GlobalRouter SW INFO Loading
   configuration
   CP1  [09/21/14 10:13:21.449] 0x00010757 00000000 GlobalRouter HW INFO Initial
   configuration download to all cards completed
   CP1  [09/21/14 10:13:21.467] 0x0003458b 00000000 GlobalRouter SW INFO The system
   is ready
   ```

Downgrading from Release 4.0 or 4.0.1

About this task

Use this procedure to downgrade to Release 3.x when a 9048XS-2 or 9012QQ-2 I/O module is installed and you are running Release 4.0.

Procedure

1. Have the Release 3.x configuration you wish to use after downgrading ready and saved on the VSP 9000.

2. High Speed Fan Trays and Switch Fabric cards can remained installed in the chassis. The High Speed Fan Trays will work with Release 3.4.x but may not be recognized if downgrading to a version prior to Release 3.4.2.2.

3. Disable and power down the 9048XS-2 or 9012QQ-2 modules. Save the configuration if you will not be booting from a saved Release 3.x configuration.
4. Remove the cards if the chassis is local.
5. Follow normal downgrade procedures.
6. The 9048XS-2 or 9012QQ-2 modules will not power on once you are running a 3.x release.

New features

The following sections highlight the feature support added in this release.

First generation and second generation mode

Release 4.0 introduces a second generation mode for Virtual Services Platform 9010 and Virtual Services Platform 9012 to support second generation modules and enhanced scaling features. The following conditions apply to both the Virtual Services Platform 9010 and the Virtual Services Platform 9012:

- First generation mode: Supports all first generation and second generation modules.
- Second generation mode: Supports only second generation modules.

Note:

For the Virtual Services Platform 9012: If you use second generation modules, you must use the 9012FCHS cooling module. The 9012FCHS cooling module cannot be used in conjunction with other cooling modules in the VSP 9012. If the 9012FCHS must be used, all cooling modules must be 9012FCHS modules.

For more information about configuring the minimum module generation mode, see *Configuring Ethernet Modules on Avaya Virtual Services Platform 9000,* NN46250-508.

For more information about the first generation and second generation modules and modes, see New hardware supported on page 17.

IS-IS accept policies

Avaya Virtual Services Platform 9000 provides the ability to use Intermediate-System-to-Intermediate-System (IS-IS) accept policies with Layer 3 VSNs or IP Shortcuts to filter incoming IS-IS route updates from the IS-IS protocol. IS-IS accept policies enable the device to determine whether to add an incoming route to the routing table. IS-IS accept policies are disabled by default.

You can create an IS-IS accept policy for the Global Routing Table (GRT) or a Virtual Routing and Forwarding (VRF) instance. You can create an IS-IS accept policy on a switch that operates at a global default level or for a specific advertising BEB. You can also use the filter mechanism for IS-IS accept policies to redistribute routes between different VRFs, or between a VRF and the GRT.

For more information about IS-IS accept policies, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 9000,* NN46250-510.

IS-IS adjacencies scaling

Release 4.0 offers enhanced scaling for IS-IS adjacencies. Support increases to 128 adjacencies, up from 64 in prior releases.

Scaling to 1 million FIB records

Release 4.0 offers enhanced scaling for IPv4 FIB routes to 1,000,000 for second generation I/O modules in second generation mode.

Change to SPB drop statistics

Virtual Services Platform 9000 does not support the **`show isis spbm drop-stats port unknown-unicast-sa`** command for second generation modules in this release. The device always displays the ACLI output for second generation modules as 0 for this counter. For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 9000,* NN46250-510 or *Monitoring Performance on Avaya Virtual Services Platform 9000,* NN46250-701.

New hardware supported

This section identifies new supported hardware.

First and second generation modules and modes

First generation and second generation modules operate in any I/O module slot in both Virtual Services Platform 9010 and Virtual Services Platform 9012.

The following table identifies the first generation and second generation module types and shows the various support configurations for each mode.

Chassis mode	Modules	Supported on both VSP 9010 and VSP 9012	High speed cooling module support
First generation mode	First generation modules: • 9024XL • 9048GB • 9048GT	• Supports all first generation modules and second generation modules. • Switch Fabric (SF) modules: - First generation modules: require a minimum of three SF modules. - Second generation modules: require a minimum of five SF modules.	• First generation modules on VSP 9010: use the 9012FC cooling module. The 9012FCHS is not required on the VSP 9010. • First generation modules on VSP 9012: use the 9012FC cooling modules or the 9012FCHS cooling modules. **Note:** Second generation modules running in first generation mode on the VSP 9012 still require the 9012FCHS cooling module.
	Second generation modules: • 9048XS-2 • 9012QQ-2		

Table continues…

Chassis mode	Modules	Supported on both VSP 9010 and VSP 9012	High speed cooling module support
Second generation mode	Second generation modules: • 9048XS-2 • 9012QQ-2	• Supports only second generation modules. • Requires a minimum of five SF modules. • Achieves enhanced scaling capabilities for FIB routes.	• Second generation modules on VSP 9010: use the 9012FC cooling module. The 9012FCHS is not required on the VSP 9010. • Second generation modules on VSP 9012: require the 9012FCHS cooling modules.

Note:

- If you install a second generation module in Virtual Services Platform 9010 or Virtual Services Platform 9012, you must have a minimum of five SF modules installed. Populate slots SF1 and SF4, and use any other slots for the remaining three SF modules.
- If you install a first generation module in Virtual Services Platform 9010 or Virtual Services Platform 9012, you must have a minimum of three SF modules installed. Populate slots SF1 and SF4, and use any other slot for the remaining SF module.
- If you install a second generation module in Virtual Services Platform 9012, you must also install the 9012FCHS cooling modules. After you insert a second generation module into Virtual Services Platform 9012, the system checks which cooling modules are in use, and if the system does not use the 9012FCHS cooling modules, the second generation modules remain offline.

First generation mode configuration

Virtual Services Platform 9000 with first generation modules are based on 3 x 48Gbps Network Processing Unit (NPU). If you want to use both first generation and second generation modules, you must use the default parameter **`gen1`** with the **`boot config linecard-compatibility-mode {gen1|gen2}`** command, which configures the system to first generation (gen1). After you configure the device for first generation modules, the system reboots in first generation (gen1) mode.

First generation mode is the default mode of operation.

Second generation mode configuration

Virtual Services Platform 9000 with second generation modules is a fully-featured high performance high-end platform based on 3 x 160Gbps NPUs per I/O module. If you want to use only second generation modules and achieve full scaling capability, you must use the parameter **`gen2`** with the **`boot config linecard-compatibility-mode {gen1|gen2}`** command, which configures the system to second generation (gen2). The system reboots in second generation mode and disables all first generation modules.

For more information, see *Configuring Ethernet Modules on Avaya Virtual Services Platform 9000,* NN46250-508.

9048XS-2 I/O module

The second generation 9048XS-2 Input/Output (I/O) module is a 48 port 10 Gigabit per second (Gbps) module. The 9048XS-2 module supports the 10GBASE-R small form-factor pluggable plus (SFP+) transceivers and the 1000BASE-X SFP transceivers. The Virtual Services Platform 9000 supports the 9048XS-2 module in first generation mode and second generation mode. The Virtual Services Platform 9012 requires the 9012FCHS I/O cooling module to be installed before you install the 9048XS-2 module. You must also have a minimum of five Switch Fabric modules installed, if you install the 9048XS-2 module on the Virtual Services Platform 9012. Populate slots SF1 and SF4, and you can use any other slots for the remaining three SF modules.

This module supports standard management information bases (MIB).

The 9048XS-2 module is oversubscribed 2:1, with full QoS awareness, with regards to line rate over 48 ports of 10 Gbps Ethernet traffic using standard SFP+ fiber transceivers. This module supports a maximum throughput of 357 Million packets per second (Mpps) over 48 ports of 10 Gbps Ethernet traffic using standard SFP+ fiber transceivers. The module supports SR, LR, LRM, ER, and ZR SFP + format.

For information about supported transceivers, see *Administering Avaya Virtual Services Platform 9000,* NN46250-600.

Note:

ZR SFP+ transceivers are limited to 12 per module. Transceivers of this type should only be used in ports 1,6,9,14,17,22,25,30,33,38,41,and 46 to ensure proper cooling.

Important:

Virtual Services Platform 9000 supports only Avaya-qualified transceivers. Other vendor transceivers will not work and Avaya does not support them.

The 9048XS-2 I/O module has a dual core P2020 processor and 2 GB onboard DDR3 memory. You can use the 9048XS-2 module in both the Virtual Services Platform 9010 and Virtual Services Platform 9012 chassis.

The 9048XS-2 has the following characteristics:

- compliant with IEEE 802.3ae standards
- 802.3 Ethernet frame format, MAC layer functionality
- 64B/66B line encoding
- asynchronous Ethernet interface

9012QQ-2 I/O module

The second generation 9012QQ-2 Input/Output (I/O) module is a 12-port 40 Gigabits per second (Gbps) module. The 9012QQ-2 module supports the 40GBASE-R QSFP+ transceivers.

The 9012QQ-2 module supports the following:

- Maximum throughput of 357 Million packets per second (Mpps) with 64 Byte packets
- standard management information base (MIB), 802.3ba
- Oversubscription of 2:1
- 80Gbps of bi-directional traffic per slice, with 240Gbps aggregate per module, assuming five Switch Fabric Modules installed

Linecard-compatibility-mode

You can use the 9012QQ-2 module in first generation or second generation linecard-compatibility-mode; however, if you want the system to configure the maximum routes to one million, you must configure the `boot config linecard-compatibility-mode {gen1|gen2}` command to second generation (gen2). After you configure the boot config linecard-compatibility-mode to second generation, the VSP 9000 chassis does not support first generation modules. For more information, see *Configuring Ethernet Modules on Avaya Virtual Services Platform 9000,* NN46250-508.

Important:

The chassis will restart every time the boot config linecard-compatibility-mode command is used. There is no way to prevent this action. Use of this command is service impacting.

Considerations

Consider the following when you use the 9012QQ-2 module:

- You must have a minimum of five Switch Fabric modules installed, if you install the 9012QQ-2 module on the Virtual Services Platform 9012.
- The Virtual Services Platform 9012 requires the High-Speed Front Cooling Modules be installed before you install the 9012QQ-2 module.
- The 9012QQ-2 module does not support Lossless Ethernet in the current release.

Existing hardware supported in the current release

Refer to these documents for information on the existing Avaya Virtual Services Platform 9000 hardware supported by the current release.

- *Installing Modules in Avaya Virtual Services Platform 9000,* NN46250-301
- *Installing Cooling Modules in Avaya Virtual Services Platform 9000,* NN46250-302
- *Installing AC Power Supplies in Avaya Virtual Services Platform 9000,* NN46250-303
- *Installing the Avaya Virtual Services Platform 9000,* NN46250-304

File names

This section describes the Avaya Virtual Services Platform 9000 software files.

Software files

The following table provides the details of the Virtual Services Platform 9000 software files.

Table 2: Software files

File name	Description
VSP9K.4.0.1.0.tgz	Release 4.0.1 archived distribution
VSP9K.4.0.1.0_modules.tgz	Encryption modules
VSP9K.4.0.1.0_mib.zip	Archive of all MIB files
VSP9K.4.0.1.0_mib.txt	MIB file
VSP9K.4.0.1.0_mib_sup.txt	MIB file
VSP9000v401_HELP_EDM_gzip.zip	EDM Help file
VSP9K.4.0.1.0.md5	MD5 Checksums

Important:

Download images using the binary file transfer.

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

Always verify the file sizes after download.

Open Source software files

The following table gives the details of the Open Source software files distributed with the Virtual Services Platform 9000 software.

Table 3: Open Source software files

File name	Description
VSP9K.4.0.1.0_oss-notice.html	Master copyright file. This file is located in the Licenses directory.
VSP9K.4.0.1.0_OpenSource.zip	Open source base software for Virtual Services Platform 9000 Release 4.0.1.

You can download Avaya Virtual Services Platform 9000 software and files, including MIB files, from the Avaya Support Portal at www.avaya.com/support.

Important information and restrictions

This section contains important information and restrictions you must consider before you use the Avaya Virtual Services Platform 9000.

Protecting modules

⚠ **Warning:**

Risk of equipment damage. Do not touch the top of the module or you can damage pins, components and connectors.

⚠ **Warning:**

Modules are heavy. Damage to a module can occur if it bumps into another object, including other modules installed in a chassis. Use both hands to support modules.

Virtual Services Platform 9000 modules are larger and heavier than Ethernet Routing Switch 8000 series modules. Handle the modules used in Virtual Services Platform 9000 with care. Take the following items into consideration when you handle modules:

- To prevent damage from electrostatic discharge, always wear an antistatic wrist strap connected to an ESD jack when you connect cables or you perform maintenance on this device.
- Always place the modules on appropriate antistatic material.
- Support the module from underneath with two hands. Do not touch components or connector pins with your hand, or damage can result.
- Damage to a module can occur if you bump the module into another object, including other modules installed in a chassis. Be careful not to bump module connectors against the action levers of an adjacent module. Damage to connectors can result. Use both hands to support modules.
- Visually inspect the connectors for damage before you insert the module. If you insert a module with damaged connectors you will damage the midplane.
- Check the clearance between the insertion lever and the gasket on adjacent modules during insertion or extraction.
- Do not stack modules one on top of the other when you move them.
- Do not leave slots open. Fill all slots with modules or filler modules to maintain safety compliance, proper cooling, and EMI containment.
- Do not over tighten screws. Tighten until snug. Do not use a power tool to tighten screws.

Module installation precautions

You must take the following precautions while you install modules in the Virtual Services Platform 9000:

- Ensure the module sheet metal slides in the rails on the side of the Virtual Services Platform 9012 chassis, or the top and bottom of the Virtual Services Platform 9010 chassis.
- Modules come with screws embedded in the sheet metal. You must use the screws to keep the cards tightly in place.
- You must support the weight of the modules until they are inserted completely.

Resetting multiple modules

When you reset multiple modules in the system, it is important to make sure the module has fully recovered before you reset the next module. If the subsequent module is reset before the previous module has recovered, various error messages can appear as the system recovers through the system synchronization.

Removing a master CP module with CPU-HA mode activated

Perform this procedure, if the system operates in CPU-HA mode, to properly remove the master CP module. You must perform this procedure to avoid jeopardizing the integrity of the file system.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Use the `sys action cpu-switch-over` command to fail over to another CP.
3. Use the slot power commands to power down the module.
4. Remove the CP module.

   This action removes the original master.

   Important:

   Do not reinsert a CP module until at least 15 seconds elapse, which is long enough for another CP module to become master.

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal

VSP-9012:1(config)#sys action cpu-switch-over
```

Removing external storage devices from the CP module

Perform this procedure to safely remove the USB and the external Compact Flash devices from the CP module. You must perform this procedure to prevent data loss or hardware damage.

Important:

Do not unplug the storage device without first performing this procedure.

You must use the appropriate stop command to unmount the device before you physically remove it from the CP module.

Before you begin

Several system tools use the external Compact Flash as the default storage location. Check the following features before you remove the card:

- Packet Capture (PCAP)
- logging
- debug or trace

The Virtual Services Platform 9000 stop command does not succeed if the specified device is in use. Common uses that impede the proper execution of the stop command are:

- USB or external Compact Flash file access is in progress (move, copy, read, or write) to or from the USB, or the external Compact Flash.

  Discontinue operations or wait for access completion before you use the stop command.

- The ACLI session current working directory is configured for the device you need to remove.

  Change the current working directory to internal Compact Flash, which is the default.

- Logging is enabled to the external Compact Flash, which is the default.

  Use the **`show logging config`** command to verify the current storage location. If the location is the external Compact Flash card that you need to remove, use the **`no logging logToExtFlash`** command to log to the internal Compact Flash.

- PCAP is enabled.

  Disable PCAP, which requires the external Compact Flash. Use the **`show pcap`** command to verify if PCAP is enabled. To disable PCAP, use the **`no pcap enable`** command.

- Debugging features are enabled.

  The debug-config file and trace-logging flags must be disabled, which is the default. Use the **`show boot config flags`** command to verify the status. Use the **`no boot config flags debug-config file`** or the **`no boot config flags trace-logging`** command to disable these flags.

About this task

Note:

Use the Avaya Compact Flash device (EC1411010-E6) with the Virtual Services Platform 9000 because the Avaya Compact Flash is validated for proper operation on the Virtual Services Platform 9000. Do not use other Compact Flash devices because they are not verified for Virtual Services Platform 9000 compatibility, and can result in loss of access to the Compact Flash device.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Remove a USB device:

   a. Unmount the USB device:

      ```
      usb-stop
      ```

   b. Wait for the response that indicates it is safe to remove the device.

   c. Physically remove the device.

3. Remove an external Compact Flash device:

   a. Unmount the external flash device:

      ```
      extflash-stop
      ```

   b. Wait for the response that indicates it is safe to remove the device.

   c. Physically remove the device.

Example

Unmount and remove the USB:

```
VSP-9012:1>enable
VSP-9012:1#usb-stop
It is now safe to remove the USB device.
VSP-9012:1#extflash-stop
It is now safe to remove the external Compact Flash device.
```

Next steps

No restrictions or requirements exist before you can reinsert a USB or external Compact Flash device. You can insert these devices at any time and Virtual Services Platform 9000 automatically recognizes them. The devices are accessible within seconds after insertion.

After you insert the external Compact Flash, enable logging to the external Compact Flash with the **`logging logToExtFlash`** command.

Additionally, you can enable the following features as required:

- PCAP
- debug-config file or trace-logging flags

Supported browsers

Virtual Services Platform 9000 supports the following browsers to access the Enterprise Device Manager (EDM):

- Microsoft Internet Explorer 8.x and 9.x
- Mozilla Firefox 28.0 and earlier supported versions

IPv4 interface MTU

Because Virtual Services Platform 9000 does not negotiate the maximum transmission unit (MTU) for IPv4 interfaces, the interface MTU is the maximum sized packet that the CP transmits. Virtual Services Platform 9000 receives and processes any packet less than the system MTU. In the fastpath, Virtual Services Platform 9000 receives and sends packets less than, or equal to, the system MTU.

For more information about the system MTU, see *Administering Avaya Virtual Services Platform 9000,* NN46250-600.

Supported system and management applications with IPv6

Note:

Virtual Services Platform 9000 does not support IPv6 configuration using ACLI or EDM for Release 4.0.

You can use IPv6 for the following access methods and features:

- DHCP Relay
- DNS client
- FTP client and server
- HTTP and HTTPS
- ping
- Rlogin
- RADIUS client
- SNMP
- SSH
- Syslog client
- Telnet
- TFTP client and server

- Traceroute

User configurable SSL certificates

Virtual Services Platform 9000 does not generate SSL certificates with user-configurable parameters. You can, however, use your own certificate.

You can generate a certificate off the VSP 9000 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 *Administering Avaya Virtual Services Platform 9000,* NN46250-600.

EDM image management

EDM does not currently support image management functionality. You must perform all image management work through the ACLI. This includes, but is not limited to, software upgrades, software image management, and software patching. See *Applying Upgrades and Patches to Avaya Virtual Services Platform 9000,* NN46250-400, for information and procedures about image management.

After you use ACLI to upgrade or downgrade the system software, before you connect to the device using EDM, Avaya recommends that you clear the browser cache. If you fail to clear the browser cache before you connect to the device, you can continue to see the previous software version in EDM.

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 *Administering Avaya Virtual Services Platform 9000,* NN46250-600.

Shutting down the system

Use this procedure to properly shut down a running system.

About this task

This command properly shuts down the file system, and powers off all I/O modules and Switch Fabric modules. The power supplies, cooling modules, and CP modules remain in the powered on state. After you use this command, you must physically turn off the chassis power. To restore power after you use this command, you must physically turn the chassis power on again.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Shut down the system:

   ```
   sys shutdown
   ```

Example

Shut down a running system.

```
VSP-9012:1>enable
VSP-9012:1#sys shutdown
Are you sure you want shutdown the system? Y/N  (y/n) ? y
CP1  [05/02/14 12:32:34.062] 0x00010813 00000000 GlobalRouter HW INFO System shutdown
initiated from CLI
SF3  [05/02/14 12:32:33.240] 0x00274597 00000000 GlobalRouter SW INFO Shutdown request
received from slot 1.
SF5  [05/02/14 12:32:33.313] 0x00274597 00000000 GlobalRouter SW INFO Shutdown request
received from slot 1.
SF2  [05/02/14 12:32:33.331] 0x00274597 00000000 GlobalRouter SW INFO Shutdown request
received from slot 1.
SF4  [05/02/14 12:32:33.399] 0x00274597 00000000 GlobalRouter SW INFO Shutdown request
received from slot 1.
SF1  [05/02/14 12:32:33.537] 0x00274597 00000000 GlobalRouter SW INFO Shutdown request
received from slot 1.
IO10 [05/02/14 12:32:36.067] 0x00274597 00000000 GlobalRouter SW INFO Shutdown request
received from slot 1.
IO6  [05/02/14 12:32:39.988] 0x00274597 00000000 GlobalRouter SW INFO Shutdown request
received from slot 1.
CP1  [05/02/14 12:32:48.064] 0x00010736 00000000 GlobalRouter HW INFO Slot 6 powered off
by admin
CP1  [05/02/14 12:32:48.066] 0x0000c5f9 00000000 GlobalRouter HW INFO Link Down(6/8)
Port disabled
CP2  [05/02/14 12:32:57.845] 0x000646fa 00000000 GlobalRouter MLT INFO IST DOWN, status
vector: 0x400000400002000
CP1  [05/02/14 12:32:58.065] 0x00010736 00000000 GlobalRouter HW INFO Slot 10 powered off
by admin
CP1  [05/02/14 12:32:58.065] 0x0000c5f9 00000000 GlobalRouter HW INFO Link Down(10/1)
Port disabled
CP1  [05/02/14 12:32:58.066] 0x0000c5f9 00000000 GlobalRouter HW INFO Link Down(10/2)
Port disabled
CP1  [05/02/14 12:32:58.068] 0x0000c5f9 00000000 GlobalRouter HW INFO Link Down(10/4)
Port disabled
CP1  [05/02/14 12:32:58.068] 0x00000009 01900001.2 DYNAMIC SET GlobalRouter SW INFO SMLT
2 Link is DOWN
CP1  [05/02/14 12:32:58.068] 0x00000009 01900001.3 DYNAMIC SET GlobalRouter SW INFO SMLT
```

```
3 Link is DOWN
CP1  [05/02/14 12:32:58.070] 0x000646fa 00000000 GlobalRouter MLT INFO IST DOWN, status
vector: 0x2060000000002800
CP1  [05/02/14 12:32:58.070] 0x000646da 01900004 DYNAMIC SET GlobalRouter MLT WARNING
SMLT IST Link is DOWN /IST Slave
CP1  [05/02/14 12:32:58.072] 0x00064708 01900005 DYNAMIC SET GlobalRouter MLT WARNING MLT
19 is OPERATIONAL DOWN
CP1  [05/02/14 12:32:58.074] 0x0000c5f9 00000000 GlobalRouter HW INFO Link Down(10/15)
Port disabled
CP1  [05/02/14 12:32:58.076] 0x00064708 01900005 DYNAMIC SET GlobalRouter MLT WARNING MLT
2 is OPERATIONAL DOWN
CP1  [05/02/14 12:32:58.077] 0x0000c5f9 00000000 GlobalRouter HW INFO Link Down(10/21)
Port disabled
CP1  [05/02/14 12:32:58.079] 0x00064708 01900005 DYNAMIC SET GlobalRouter MLT WARNING MLT
3 is OPERATIONAL DOWN
CP1  [05/02/14 12:32:58.565] 0x00010736 00000000 GlobalRouter HW INFO Slot SF 5 powered
off by admin
CP1  [05/02/14 12:32:59.066] 0x00010736 00000000 GlobalRouter HW INFO Slot SF 4 powered
off by admin
CP1  [05/02/14 12:32:59.567] 0x00010736 00000000 GlobalRouter HW INFO Slot SF 3 powered
off by admin
CP1  [05/02/14 12:33:00.068] 0x00010736 00000000 GlobalRouter HW INFO Slot SF 2 powered
off by admin
CP2  [05/02/14 12:33:00.337] 0x00274597 00000000 GlobalRouter SW INFO Shutdown request
received from slot 1.
CP1  [05/02/14 12:33:00.569] 0x00010736 00000000 GlobalRouter HW INFO Slot SF 1 powered
off by admin
CP1  [05/02/14 12:33:01.091] 0x000045b7 00000000 GlobalRouter SNMP INFO HA-CPU: Lost
connection to Standby CPU.
CP1  [05/02/14 12:33:10.000] LifeCycle: INFO: Stopping all processes
CP1  [05/02/14 12:33:11.000] LifeCycle: INFO: All processes have stopped
CP1  [05/02/14 12:33:11.000] LifeCycle: INFO: Un-mounting filesytems
CP1  [05/02/14 12:33:11.000] LifeCycle: INFO: File systems un-mounted
CP1  [05/02/14 12:33:11.000] LifeCycle: INFO: All applications stopped. It is now safe to
power down the chassis
```

SPB on an Interswitch Trunk

It is recommended that the Interswitch MLT be configured as an IS-IS interface when SPB is configured on an Interswitch Trunk (IST).

Lossless Ethernet

Virtual Services Platform 9000 supports Lossless Ethernet on first generation modules, which include: 9024XL, 9048GB, and 9048GT.

VSP 9000 does not support Lossless Ethernet on second generation modules for Release 4.0, or 4.0.1. Do not use these releases if you must use this feature on second generation modules.

IST cluster deployments

IST cluster deployments with a mixture of first and second generation I/O modules, and where the IST ports are configured on the second generation modules, ARP entries may incorrectly point traffic toward the IST MLT when they should be pointing toward the SMLT on which it was learned, resulting in dropped packets. Cluster deployments with only one module type deployed (first or second generation) will not experience this issue.

IST ports must **only** be configured on first generation I/O modules in these mixed module deployments. This is a temporary limitation that will be addressed in a follow-on maintenance release.

Fixes from previous releases

The Virtual Services Platform 9000 Software Release 4.0.1 incorporates all fixes from prior releases, up to and including, Release 3.4.3.0.

Hardware and software compatibility

Hardware and software compatibility information can be obtained from *Administering Avaya Virtual Services Platform 9000,* NN46250-600. Refer to that document for more information.

Other documents

In addition to the product documentation, Avaya provides Technical Configuration Guides and Technical Solution Guides. You can refer to these guides for more information about how to configure or use the Virtual Services Platform 9000 in specific scenarios. The following table lists the guides available for the Virtual Services Platform 9000.

Document title	Document number
Link Aggregation Control Protocol (LACP) 802.3ad and VLACP for VSP and ERS Technical Configuration Guide	NN48500-502
Switch Clustering using Split-MultiLink Trunking (SMLT) with VSP 9000, ERS 8600/8800, 8300, and 5000 Technical Configuration Guide	NN48500-518
Switch Clustering Supported Topologies and Interoperability with Virtual Services Platform 9000 & Ethernet Routing Switches	NN48500-555
Technical Configuration Guide for Microsoft Network Load Balancing	NN48500-593
Super Large Campus Technical Configuration Guide	NN48500-609
Avaya Virtual Services Platform 9000 with Coraid EtherDrive SRX-Series Storage Appliances Technical Configuration Guide	NN48500-611
Avaya Flare™ for Avaya Data Technical Configuration Guide	NN48500-613

Table continues…

Document title	Document number
Shortest Path Bridging (802.1aq) for ERS 8800 and VSP 9000 Technical Configuration Guide	NN48500-617
Migrating to a Virtual Services Fabric using Shortest Path Bridging Technical Configuration Guide	NN48500-622
Avaya Virtual Services Platform 9000 and Avaya Virtual Services Platform 7000 with Coraid EtherDrive SRX-Series Storage Appliances Technical Configuration Guide	NN48500-629
Basic SPB Configuration	NN48500-632
IPv6 for VSP 9000 Technical Configuration Guide	NN48500-634

You can find these documents at www.avaya.com/support under the product Data Networking Solution, or by performing a search.

Chapter 4: Software and hardware scaling capabilities

This chapter details the software and hardware scaling capabilities of Avaya Virtual Services Platform 9000. The information in *Release Notes for Avaya Virtual Services Platform 9000,* NN46250-401, takes precedence over information in other documents.

Hardware scaling capabilities

This section lists hardware scaling capabilities of Avaya Virtual Services Platform 9000.

Table 4: Module capabilities

Component	Maximum number supported
9012QQ-2 I/O module	
40 GbE fiber connections	9010 chassis: 96 (8 x 12) 9012 chassis: 120 (10 x 12)
Processor	800 MHz dual core
9024XL I/O module	
10 GbE fiber connections	9010 chassis: 192 (8 x 24) 9012 chassis: 240 (10 x 24)
Processor	1 GHz
9048XS-2 I/O module	
10 GbE fiber connections	9010 chassis: 384 (8 x 48) 9012 chassis: 480 (10 x 48)
Processor	800 MHz dual core
9048GB I/O module	
GbE fiber connections	9010 chassis: 384 (8 x 48) 9012 chassis: 480 (10 x 48)
Processor	1 GHz

Table continues…

Component	Maximum number supported
9048GT I/O module	
10/100/1000 copper connections	9010 chassis: 384 (8 x 48) 9012 chassis: 480 (10 x 48)
Processor	1 GHz
9080CP module	
Processor	1.33 GHz
Console port	1 D-subminiature 25-pin shell 9 pin connector (DB9) per CP module
Ethernet management	1 Registered Jack (RJ) 45 per CP module
USB port	1 Universal Serial Bus (USB) Type A (Master) per CP module
External Compact Flash	1 per CP module

Table 5: VSP 9010 AC chassis capabilities

Component	Maximum number supported
CP modules	2
Interface modules	8
SF modules	6 If you install only first generation I/O modules, you must install a minimum of three SF modules in the chassis. If you install second generation I/O modules, you must install five SF modules. Always install an SF module in both slots SF1 and SF4.
Power Supplies	8
Total power capacity	• 21.8 kW when connected to 220 VAC • 16 kW when connected to 110 VAC
Jumbo packets	9600 bytes for IPv4 9500 bytes for IPv6

Table 6: VSP 9012 chassis capabilities

Component	Maximum number supported
CP modules	2
Interface modules	10
SF modules	6 If you install only first generation I/O modules, you must install a minimum of three SF modules in the chassis. If you install second generation I/O

Table continues…

Component	Maximum number supported
	modules, you must install five SF modules. Always install an SF module in both slots SF1 and SF4.
Auxiliary slots	2
Power supplies	6
Total power capacity	• 16.3 kW when connected to 220 VAC • 12 kW when connected to 110 VAC
Jumbo packets	9600 bytes for IPv4 9500 bytes for IPv6

Software scaling capabilities

This section lists software scaling capabilities of Avaya Virtual Services Platform 9000.

Table 7: Software scaling capabilities

	Maximum number supported
Layer 2	
IEEE/Port-based VLANs	4,084
Inter-Switch Trunk (IST)	1 group
Internet Protocol (IP) Subnet-based VLANs	256
LACP	512 aggregators
LACP ports per aggregator	8 active and 8 standby
Lossless Ethernet	2 ports for each 8–port cluster 6 ports for each 9024XL module **Note:** VSP 9000 supports Lossless Ethernet on first generation modules, which include: 9024XL, 9048GB, and 9048GT modules. VSP 9000 does not support Lossless Ethernet on second generation modules.
MACs in forwarding database (FDB)	128K
Multi-Link Trunking (MLT)	512 groups
Multiple Spanning Tree Protocol (MSTP)	64 instances
Protocol-based VLANs	16
Rapid Spanning Tree Protocol (RSTP)	1 instance
SLPP	500 VLANs

Table continues…

	Maximum number supported
Source MAC-based VLANs	100
Split Multi-Link Trunking (SMLT)	511 groups plus 1 IST MLT
SMLT ports per group	16
VLACP Interfaces	128
Layer 3	
Address Resolution Protocol (ARP) for each port, VRF, or VLAN	64,000 entries total
BGP peers	256
BGP Internet peers (full)	3
BGP routes	1.5 million
BGP+ routes	128,000 **Note:** VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
Circuitless IP interfaces	256
ECMP routes	64,000
ECMP routes (fastpath)	8
FIB IPv4 routes	400,000 for first or second generation I/O modules in first generation mode. 1,000,000 for second generation I/O modules in second generation mode.
FIB IPv6 routes	128,000 for first or second generation I/O modules in first generation mode. 256,000 for second generation modules in second generation mode. **Note:** VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
The fastpath forwarding table uses a common table for IPv4 and IPv6 forwarding records. IPv6 records are approximately four times the size of IPv4 records. • For first or second generation modules in first generation mode: The maximum number of 400,000 IPv4 routes is possible when no other IPv6 routes are configured, and the maximum number of IPv6 routes is 128,000 when no IPv4 routes are configured. • For second generation modules in second generation mode: The maximum number of 1,000,000 IPv4 routes is possible when no IPv6 routes are configured, and the maximum number of IPv6 routes is 256,000 when no IPv4 routes are configured.	

Table continues…

	Maximum number supported
Note: VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.	
IPv4 interfaces	4,343
IP interfaces (Brouter)	480
IP prefix entries	25 000
IPv4 prefix list	500
IP routing policies	500 for each VRF 5,000 for each system
IPFIX flows	96,000 for each interface module 960,000 for each chassis
IPv4 or IPv6 FTP sessions	4 each, 8 total **Note:** VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
IPv4 or IPv6 Rlogin sessions	8 each, 16 total **Note:** VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
IPv4 or IPv6 SSH sessions	8 total (any combination of IPv4 and IPv6 up to 8) **Note:** VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
IPv4 or IPv6 Telnet sessions	8 each, 16 total **Note:** VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
IPv4 VRF instances	512
IPv6 dynamic neighbors/interface	64K **Note:** VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
IPv6 interfaces	4,087 (4,084 VLAN and 3 management [1/1, 2/1, virtual IP])

Table continues…

	Maximum number supported
	Note: VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
IPv6 routes (fastpath)	128,000 **Note:** VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
IPv6 static neighbors	1,000 **Note:** VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
IPv6 static routes	10,000 **Note:** VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
IPv6 tunnels	2,000 **Note:** VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
Multicast IGMP interfaces	4,084
Multicast IGMP instances	on 64 VRFs
Multicast source and group (S, G)	6,000 for each system, including VRFs
NLB Clusters — Multicast, with multicast MAC flooding disabled	1 for each VLAN 2,000 for each system
NLB Clusters — Multicast, with multicast MAC flooding enabled	128 for each VLAN 2,000 for each system
NLB Clusters — Unicast	128 for each VLAN 2,000 for each system
OSPF adjacencies	512
OSPF areas	12 for each OSPF instance 80 for each system
OSPF instances	64 (one per VRF)
OSPF interfaces	512 active, 2000 passive
OSPF LSA packet size	Jumbo packets
OSPF routes	64,000

Table continues…

	Maximum number supported
OSPFv3 adjacencies	512
OSPFv3 adjacencies per interface	256
OSPFv3 areas	64
OSPFv3 passive interfaces	1,000
OSPFv3 routers per area	250
OSPFv3 routes	64,000
PIM interfaces	512 active; 4084 passive
PIM instances	on GRT only
RIB IPv4 routes	3 * fastpath routes
RIP instances	64 (one for each VRF)
RIP interfaces	200
RIP routes	2,500 for each VRF 10,000 for each system
RSMLT interfaces (IPv4/IPv6)	4,000 over 512 SMLT interfaces **Note:** VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
Static ARP entries	2,048 for each VRF 10,000 for each system
Static routes (IPv4)	2,000 for each VRF 10,000 total across VRFs
UDP/DHCP forwarding entries	512 for each VRF 1,024 for each system
VRRP interfaces (IPv4)	255 for a VRF 512 for a system
VRRP interfaces (IPv6)	255 for a system **Note:** VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
VRRP interfaces fast timers (200ms)	24
Diagnostics	
Mirrored ports	479
Remote Mirroring Termination (RMT) ports	32
Filters and QoS	
Flow-based policers (IPv4 and IPv6)	16,000

Table continues…

	Maximum number supported
	Note: VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
Port shapers (IPv4 and IPv6)	480 **Note:** VSP 9000 does not support IPv6 in Release 4.0 and Release 4.0.1.
Access control lists (ACL) for each chassis (IPv4)	2,048 The current release does not support IPv6 filters.
Access control entries (ACE) for each chassis (IPv4)	16,000
ACEs per ACL (a combination of Security and QoS ACEs)	1,000
Unique redirect next hop values for ACE Actions (IPv4)	2,000
SPBM	
ARP entries (routed)	64,000
MAC entries	128,000 (combination of ARP entries and Layer 2 MACs)
Backbone MAC	1,000
IP routes in the Global Router	100,000 (combination of OSPF and IS-IS)
IS-IS adjacencies	128
Layer 2 VSNs	4,000
VLANs in VRF	1,600
Layer 3 VSNs	512

Chapter 5: Known issues and limitations

This section details the known issues and limitations of the Avaya Virtual Services Platform 9000. Where appropriate, use the workarounds provided.

Known Issues

Alarm, logging, and error reporting

Table 8: Known issues

Issue number	Description	Workaround
wi01004076	You can see the following error message when you boot the VSP 9000: `HW ERROR framework_process_entity_data : Application Sync failed for entity:0x414c524d representing Module ALARM`	This message has no functional impact and can be ignored.

wi01057618	Occasionally, the following error messages may appear on the console:
	`IO6 [11/02/12 15:04:12.255] 0x00170563 00000000 GlobalRouter COP-SW ERROR K2-2 PCIE_BAD_ADR INT Event, bad address = 0x12fb8a6c`
	`IO6 [11/02/12 15:04:12.255] 0x00170566 00000000 GlobalRouter COP-SW WARNING K2-2 CMD PKT Logic Error: REPLY CODE=0x80`
	`IO6 [11/02/12 15:04:12.255] 0x00170574 00000000 GlobalRouter COP-SW ERROR`
		These messages do not impact the operation of the switch and can be ignored.

Table continues…

Issue number	Description	Workaround

	`K2-2 Zag-1 BAP I/F Error Adr = 0x70, Data = 0x2000`
	`IO6 [11/02/12 15:04:12.255] 0x00170574 00000000 GlobalRouter COP-SW ERROR K2-2 Zag-1 BAP I/F Error Adr = 0x74, Data = 0x20b8a6c`
	`IO6 [11/02/12 15:04:12.255] 0x001705fb 00000000 GlobalRouter COP-SW ERROR K2-2 Zag-1 BAP RSP reg 0x1C: 0x402 0xD4: 0x10 0xD8: 0x20b8a6c`
	`IO6 [11/02/12 15:04:12.255] 0x00118526 00000000 GlobalRouter COP-SW ERROR @/vob/cb/nd_dld/cbio/rlcd/lib/rlcd_util.c#574:rspRead32() k2b_pci_read failed rc: -1!!, k2DevId: 6, k2Slice: 2`	

wi01092935	In some scenarios, you can see the following error message: `CP2 [04/10/13 17:40:24.533] 0x0001079a 00000000 GlobalRouter HW ERROR framework_process_entity_data : Application Sync failed for entity:0x4952534d representing Module IRSM ,event:4/4 maxNumEvents: 11.`	This causes no negative issue.
wi01168372	The memory used to store RMON information is shared between alarms and events. The maximum number of each is dependent on the number of alarm-event pairs configured.	—
wi01183021	A log message may be encountered with the text "GlobalRouter COP-SW WARNING K2-0". This message is not service impacting and can be ignored.	—
wi01200901	Users may experience an outage when adding a module to a live chassis.	—

Table continues…

Issue number	Description	Workaround
wi01207750	Layer 3 remote mirroring may not work when monitoring destinations on SMLT VLANs.	Users should have the Layer 3 mirroring destination connected on a seperate VLAN. This VLAN should not span on multiple switches.
wi01207826	Layer 3 flow mirroring does not take precedence over port mirroring on second generation I/O modules. The mirror destination will receive both copies from port and flow mirroring.	

Chassis operations

Table 9: Known issues

Issue number	Description	Workaround
wi00564595	If there is not enough power available in the chassis to power all cards when the system is powered up, one or more cards will not be powered on. Configuration for these cards will be ignored. When enough power is available the cards will be automatically powered up but they will not automatically receive their configuration.	To download the configuration to any cards that experience delayed boot up, source the configuration for that card.
wi00891718	Unable to access `/usb` from the peer CP.	Use TFTP from the peer or configure the network management port and use a transport protocol like FTP or TFTP, directly to the secondary CP.
wi00969922	If you remove the backup CP module, you can see the following output on the console: `fbuf allocated in "/vob/cb/nd_platform/chassis/lib/ch_sync.c" at line 341 is freed` This message occurs if an application tries to synchronize data to the backup CP module at the same time that you remove the module.	This message has no functional impact and can be ignored.
wi00970236	The default value for the loadingconfig time is 15 minutes. The configurable range for the **`boot config`**	Beginning with Release 4.0, the **`boot config loadconfigtime`** command is no longer supported.

Table continues…

Issue number	Description	Workaround
	`loadconfigtime` command is 0 to 300 seconds. If you configure a value that is less than the default, the device still uses the default value to validate the loading time. Because the maximum configurable value is 300 seconds, the value is always less than the default and does not take effect. The intent of the parameter is the time to load the configuration. The timer that runs in the VSP 9000 actually tracks the full start time, for example, the time spent waiting for other IO ready and to download port MAC.	
wi01096199	When a chassis is rebooted and comes up, all modules must be “online” and “ready” before the Chassis Manager decides to download the configuration. If a module is not ready at that time, then it will be left out and “hot-inserted” at a later point. Configuration for that module will be lost, and the module will be loaded with the default configuration.	Make sure all modules are up and operational, and then source the configuration file.
wi01123043 and wi01127303	In rare circumstances, when powering down a chassis, for example, a chassis reboot or software upgrade, there may be a crash on shutdown due to a small timing window when cleaning up a particular process. This does not affect any services as it powers up, nor does it have any effect on the boot-up.	—
wi01130808	The **`show sys-info temp`** command does not show Zone 5 for CP modules. This is a display issue and there is no impact to thermally driving the chassis. The hottest and coolest are still properly recorded and driving the chassis thermals/fan.	This is a display issue. You can gauge system thermal health of the CP by using the other outlet sensor.
wi01190901	An outage may be observed when a module is added to a running chassis and that module is defined in the configuration file. No outage occurs if the module is not yet defined in the configuration file.	—

EDM

Table 10: Known issues

Issue number	Description	Workaround
wi00948868	EDM can take a significant amount of time to capture and display the MAC and ARP table with the maximum number of 128K MAC and 64K ARP entries.	—
wi00956046	You cannot use FireFox 7.x to connect to an IPv6 address with HTTPS. The connection appears as untrusted, and if you select the option to add a security exception, the browser displays an error. This issue is a known Mozilla bug (633001).	Use FireFox 3.x or Internet Explorer.
wi00965260	Do not use **VLAN** > **VLANs** > **IP** > **RSMLT** tab to configure RSMLT hold-down timer and hold-up timer parameters for IPv6.	Use **IPv6** > **RSMLT**to configure the IPv6 only interface RSMLT hold-down timer and hold-up timer interfaces.
wi01047577	EDM should show OSPF interfaces on the neighbor tab. The neighbor tab should clearly mention neighborIPAddr [NBRIPADDR] and Neighrouterid [NBRROUTERID]. Currently, the tab shows IPADDR; whether it is an OSPF interface address or neighbor interface address is missing in the EDM display.	Use **`show ip ospf neigh`** in ACLI.
wi01081155	The DC OK LED does not display status in EDM. The 9006AC power supply in the chassis does light this LED to display status.	—
wi01113706	Time-out dialog boxes can appear when you launch the MgmtRouter context with a loaded configuration, for example, 128 SMLT and 4,082 VLANs. There is no impact on functionality.	—
wi01155021	OpenSSL implementation does not support AES encryption from most browsers.	—
wi01202035	Multiple route maps may be displayed in EDM when only one should be displayed.	—

HA operations

Table 11: Known issues

Issue number	Description	Workaround
wi00937861	The **exception dump max-disk-space** configuration ACLI command is not available on the standby CPU.	—
wi01106991	The following messages appear on the master CP console of an HA switch when you scale 255 VRRP interfaces on SMLT VLANs of an IST peer under one VRF: `SW WARNING smltProcLearnMacAddrWithLifid VRRP BACKUP_MASTER is ENABLED and Mac is VRRP_SRC_MAC. Do NOT learn it on IST MGID CP2 [06/13/13 14:26:28.655] 0x00000658 00000000 GlobalRouter SW WARNING smltDumpLearnMacAddrLifidMsgmac 00:00:5e:00:01:37 Vlan 255 portType 1 smlt 65535 port 111 status 0 ip 0.0.0.0 lastMac 0LifId 0 Lpid 0` After configuration, all 255 VRRP interfaces are UP on both IST peer switches.	This warning appears due to an occasional race condition while configuring VRRP. There is no traffic loss, service impact, or side effects.
wi01162570	Users may observe the following error during HA operations: `0x000b45ba 00000000 GlobalRouter SW ERROR rtmChangeListSyncCallback: vrfId: 0 received entry can't be located` This is a temporary error that can be ignored.	—
wi01188623	The HA state may be displayed incorrectly.	—
wi01196226	Users may see extended heartbeat errors during table sync on first HA failover with scaled BGP routes.	—

Table continues…

Issue number	Description	Workaround
wi01201467	IGMPv3 traffic loss can occur during a High Availability failover.	—
wi01207149	Users may observe a VSPTALK back trace during a failover in warm standby mode. There is no service impact from this action.	—

Hardware

Table 12: Known issues

Issue number	Description	Workaround
wi01102332	VSP 9000 interface modules have a high-profile, high-compression gasket that extends a very short distance above the edge of the front panel sheet metal. Some care needs to be taken to make sure that the insertion lever does not catch the gasket.	Check the clearance between the insertion lever and the gasket on adjacent modules during insertion or extraction. Also, inserting cards from bottom up makes this easier as per details in *Installing Modules in Avaya Virtual Services Platform 9000,* NN46250-301.
wi01181840	Remote fault indication detection is incorrectly reported through the front panel LED as a Local fault.	—
wi01213851	In rare cases, LEDs may erroneously report a link fault when physical connectivity is first established.	Disable and re-enable the port to clear the issue.

Management and general administration

Table 13: Known issues

Issue number	Description	Workaround
wi00509904	File transfer may fail when attempting to move large files with TFTP.	Use FTP for transfer of files larger than 32MB.
wi00510551	Compression options are not supported in SSHv2 but no error message is displayed when they are used.	Do not use compression options with SSHv2.
wi00520113	Transferring files using passive FTP may fail when using a Windows PC.	Use active mode when transferring files with FTP.

Table continues…

Issue number	Description	Workaround
wi00979353	The ACLI command to configure the SNMPv3 trap target entry does not support the entry name configuration. The name is derived internally from the IP address and port number by using the MD5 hash. If you use EDM to create the trap target entry, the specified entry name is not retained after you use the `save config` command and restart the system. The name will be derived from the host IP address and port number.	—
wi01109195	The system does not support filenames that contain a colon (:).	Do not use a colon in filenames on the system.
wi01122342	If you create a default route in the Management VRF and create an FTP connection to the Global Routing Table VRF IP address, the outgoing FTP transfer data will go out the Management VRF.	Avaya recommends that you do not configure a default route in the Management VRF and instead use a static route. For more information about the Management VRF and static routes, see *Configuring IP Routing on Avaya Virtual Services Platform 9000,* NN46250-505. If by mistake you do get into this situation, on the host where you initiate FTP, set FTP to passive.
wi01129311	If you create a port mirroring instance and the monitoring destination is monitor VLAN, and the monitor VLAN has 3/1 as a port member, you will not see mirrored packets on 3/1. All other ports in the monitor VLAN will receive the mirrored packet.	If the mirrored packets must go out on 3/1, use the out-port parameter.
wi01164854	The command `show pluggable-optical-modules` may display inaccurate information.	—
wi01177026	IPFIX flow entries are not displayed for the 9048XS-2 I/O module in the ACLI.	—
wi01177192	IPFIX hash statistics are not displayed for the 9048XS-2 I/O module.	—
wi01177518	The command `ip ipfix template-refresh-packets` does not work with the 9048XS-2 I/O module.	—

Table continues…

Issue number	Description	Workaround
wi01178561	IPFIX flow records are not grouped in an export packet on 9048XS-2. Only one flow record per IPFIX export packet.	—
wi01177926	IPFIX flow information packets may not be captured according to the configured sample rate on the 9048XS-2 I/O module.	—
wi01190609	With IPFIX enabled, there can be packet loss seen at high traffic rates. If IPFIX is required, set the sample rate to a value below 50.	—
wi01190660	IPFIX does not show the egress port in flow packets if the egress port is part of an MLT.	—
wi01193995	The password prompt is displayed after entering a pass-phrase when authentication is set to pass-phrase only.	—
wi01194506	Both management IPs must be configured to use the virtual management IP.	—
wi01195052	The initial NTP synchronization after boot up can take up to 15 minutes.	—
wi01196660	EAPoL requests sent to the RADIUS Server regardless of whether RADIUS is globally enabled or not.	Remove the RADIUS server EAPoL entry from the configuraton.
wi01196662	EAPOL is not logging a message when dynamic VLAN assignment occurs.	—
wi01202461	An error message may be displayed when deleting a file whose name contains a colon.	—
wi01206147	Users may experience failures in mibwalk when two IPFIX collectors are configured and the IP address of the first collector is higher than the IP address of the second collector.	Delete the first collector.
wi01207160	The ACLI command **`show pluggable-optical-modules details`** displays all four channels of information for a 40GB QSFP. The equivalent EDM screen only displays one channel.	Use the ACLI command to display the complete set of information.

Table continues…

Issue number	Description	Workaround
wi01208627	Users we may not see the control packets transmitted by the CP in the capture buffer when PCAP is enabled at the port level.	Use port mirroring to capture these packets.
wi01211531	Users may see errors in their logs files in rare instances when the number of log files in storage is greater than 999.	Regularly delete old log files so there are less than 999 files in storage.

MLT, SMLT, and link aggregation

Table 14: Known issues

Issue number	Description	Workaround
wi00822560	Disable member ports before deleting an MLT.	—
wi01169208	Users may experience unexpected behavior if they disable STP on one end of an MLT with LACP enabled.	—
wi01196289	Users may experience errors when downgrading SMLT ports.	—

Multicast

Table 15: Known issues

Issue number	Description	Workaround
wi01115976	The system cannot filter specific senders and allow other senders to transmit on IGMPv2 enabled interfaces.	Use IGMPv3 for control plane restrictions or use ACL filters.
wi01128586	On interfaces enabled for Layer 3 VSN with Multicast (Layer 3 Multicast over Shortest Path Bridging), IGMP V2 hosts requesting membership for group addresses in the Source Specific Multicast range (SSM) will not work properly if the IGMP version of the interface is 1 or 2.	This issue has 3 workaround scenarios: 1. IGMP V2 SSM range membership reports are fully supported on Layer 3 VSN Multicast interfaces by configuring the interface as follows: a. Set the IGMP version of the Layer 3 VSN multicast interface to 3. b. Enable `ip igmp compatibility-mode`.

Table continues…

Issue number	Description	Workaround
		2. The IGMP SSM range on the VRF is configurable and can be configured to restrict the SSM range to just one un-used multicast group address. Thus, all but this one group address will be in the non-SSM range, and any IGMPV2 membership group with non-SSM range address will be processed with no traffic loss. 3. The SSM range group can be configured as an IGMP static group entry for an outgoing port. This configuration will allow IGMPV3 membership with the static SSM group range to be processed with no traffic loss. For example, under the VLAN Interface Configuration mode: `(config-if)#`**`ip igmp static-group 232.1.1.1 232.1.1.2 6/1 static`**
wi01193274	Invalid group displayed on console after a CPU switch over.	—

Patching and upgrading

Table 16: Known issues

Issue number	Description	Workaround
wi00511642	The **`software patch commit`** and **`software patch remove`** commands will not display messages such as Syncing release directory on backup CP card in slot 2 while executing the command in a Telnet session.	—
wi00888516	If you apply multiple patches using the patch-id parameter, and at least one patch is a candidate and at least one patch is a non-candidate, the system returns an error message. The error message identifies the non-candidate patch but does not indicate the other	Use the **`show software patch`** command to see the status of the patches.

Table continues…

Issue number	Description	Workaround
	patches were applied, even though they were.	
wi01115509	Do not wait for the software to auto-commit a reset patch. The auto-commit feature waits 240 minutes to commit a reset patch.	When you apply a reset patch, you must manually commit the patch after the chassis restarts.
wi01129127	While adding a version of software prior to VSP 9000 Release 3.4 to the system, the following message appears: `Unable to update release information for release X.` A new accounting feature was added to VSP 9000 Release 3.4 that tracks when a software release was added, activated, and committed. This feature is only supported on VSP 9000 Release 3.4 and later. During the software add of a prior release, the system cannot update the database because the database is not present in prior releases.	This error message does not affect the add or activation of a prior VSP 9000 release and can be safely ignored.
wi01217421	When a unicast Address Resolution Protocol (ARP) response packet from the edge traverses through a 9024XL module, a 9048GT module, or a 9048GB module to a 9048XS-2 module, or a 9012QQ-2 module interswitch trunk (IST) multilink trunk (MLT), the special packet processing of ARP is not handled correctly. This led to an ARP request pointing to the IST cluster on one side and split multilink trunk (SMLT) on the local side, causing traffic issues. The patch is hitless, but the module has to power off, and then on again, for the new RSP image to be loaded.	1. Use the **`show software`** command to verify that the software load label on the chassis is 4.0.1.0.GA, which is the primary release. If the software label is not 4.0.1.0.GA do not proceed with the patch application and contact your next level of support. 2. FTP the patch file VSP9K.4.0.1.0.GA-T01217421A.tgz to the /intflash in binary format. **Note:** Please ensure that the syncing of information to the backup CP module is complete before you proceed to the next step. 3. Ensure you are in Privileged EXEC mode, or higher, in ACLI. Use the **`software patch add VSP9K.4.0.1.0.GA-T01217421A.tgz`** command to add the patch.

Table continues…

Issue number	Description	Workaround
		4. Use the **`show software patch`** command to ensure the patch status reads: “ca”. 5. Use the **`software patch apply patch-ids T01217421A`** command to apply the patch. 6. Use the **`show software patch`** command to ensure the patch status reads: “ap”, 7. Use the **`software patch commit`** command to commit the software. 8. Use the **`show software patch`** command to ensure the patch status reads: “ap”. 9. The module has to power cycle off, and then on, for the new RSP image to take effect. Ensure you are in Global Configuration Mode in ACLI, and then, use the **`no sys power slot {slot[-slot][,...]}`** command for the particular slot to power off, followed by the **`sys power slot {slot[-slot][,...]}`** command, to power on the module. Now the new RSP image takes effect. **Note:** If you wish to remove the patch, enter the following commands in the following order to remove the patch: 1. `software patch revert patch-ids T01209683A` 2. `software patch commit` 3. `software patch remove version 4.0.1.0.GA patch-id T01209683A` 4. `show software patch`

Routing

Table 17: Known issues

Issue number	Description	Workaround
wi01028980	When booting with a configuration that contains duplicate IPv6 addresses on an SMLT VLAN, Duplicate Address Detection (DAD) fails and shows the preferred IPv6 address instead of Duplicate.	If you update the configuration, Duplicate Address Detection will work. Do not use the same address for RSMLT peers in the configuration file.
wi01082088	`OSPF INFO HA-CPU LSDB sanity check: AS external checksum total mismatch` log message is changed from Warning to Info.	This message indicates an internal error condition of a record, but has no functional impact, and OSPF operates correctly if an HA failover is performed. However, to investigate further perform the following: 1. Obtain **`show ip ospf ase`** information from both Master and Standby CPs. 2. Compare output: a. If only self-originated LSAs are out of sync with sequence number, then reset the Standby CP. b. If any LSAs are not self-originated and out of sync (disregard the age column), contact Avaya Support to report this issue.
wi01091347	In a dual CP configuration, if the OSPF Router ID is detected to be the same as another OSPF router, multiple framework sync error messages can appear on the Primary CP console window: `CP2 [04/04/13 07:22:51.191] 0x0001079a 00000000 GlobalRouter HW ERROR framework_process_entity_data: Application Sync failed for entity:0x4f535046.` These framework sync errors indicate a problem syncing the duplicate Router ID	This condition is a misconfiguration in the network and very rare. If this condition occurs, enable tracing for OSPF to see the trace log for the hello packet received that has the same Router ID. Correct the other Router ID to be unique and these framework sync error messages will not appear.

Table continues…

Issue number	Description	Workaround
	information to the Secondary CP, which is correct. There is no functional impact caused by these messages. Users can still create a Telnet connection to the switch and manage it. OSPF is working properly and not allowing a neighbor adjacency to form with the duplicate OSPF Router ID.	
wi01122597	**`show ip arp`** does not show the total number of ARP entries for the current VRF.	If you want to see an ARP summary per VRF, including the current VRF, use **`show ip vrf`**.
wi01126460	The VSP 9000 does not support less specific static routes with a global next-hop address that falls within the route being configured. For example: 2000::0/48 with next hop 2000::1 will be blocked even though the next hop addresss 2000::1 may be reachable with a more specific route.	Always configure static routes with a link-local next hop instead of global.
wi01134134	ACL filters with the default deny action and permit control-packet-action not working after a line card powers off and on.	Use the command **`filter acl set 30 default-action deny control-packet-action permit`** to restore functionality.
wi01163533	Highly scaled OSPF routes may not be advertised properly.	—
wi01164891	Timers cannot be configured between BGP peer groups.	—
wi01169460	When a BGP neighbor is applied with a outbound route map set with as-path prepend, the new as-path is not prepended to the permitted routes	—
wi01179396	Bytes count is not displayed in the **`show filter acl statistics ACL# ACE#`** command when applied to a 9048XS-2 I/O module.	—
wi01190374	BGP is not supported in COM 3.1.	—
wi01192436	The MLT up/down trap is not sent when the first port of the MLT transitions up or the last port of the MLT transitions down.	Log messages of the MLT up and down events are written and sent to syslog servers if configured.
wi01197696	The switch fabric does not load balance when the ingress port is on a legacy module and the egress port is a 40GB port. All the traffic egresses 1 switch fabric port which limits the throughput to	—

Table continues…

Issue number	Description	Workaround
	the fabric port speed. This is an expected behavior.	
wi01195036	Filtered routes are removed from both the RTM and ip-unicast fib entry.	—
wi01202750	An error message is displayed when trying to delete ports from a disabled ACL.	—
wi01206135	Spoof detection does not work with the VRRP virtual IP address.	—
wi01206320	Users may observe a port bounce in the log when inserting a 40GB DAC cable.	—
wi01207496	The **Match Protocol > ISIS** option is not available in EDM when creating a new policy on the **IP > Policy > Route Policy** screen.	Use the equivalent ACLI commands to perform this procedure.
wi01217238	IST cluster deployments with a mixture of first and second generation I/O modules, and where the IST ports are configured on the second generation modules, ARP entries may incorrectly point traffic toward the IST MLT when they should be pointing toward the SMLT on which it was learned, resulting in dropped packets. Cluster deployments with only one module type deployed (first or second generation) will not experience this issue.	IST ports must **only** be configured on first generation I/O modules in these mixed module deployments. This is a temporary limitation that will be addressed in a follow-on maintenance release.

SPBM and IS-IS

Table 18: Known issues

Issue number	Description	Workaround
wi01004034	The ERS **`show isis spbm show-all`** command is not available on VSP 9000.	—

wi01109764	In a highly-scaled Layer 2 VSN (IGMP snooping) multicast over SPB configuration on an IST peer router, if IS-IS is disabled globally on both IST peers, and then re-enabled, the following error log can appear:	Disable and re-enable IGMP snooping. Perform the following in ACLI:
		`# config terminal`
		`(config)# interface vlan 100`
		`(config-if)# no ip igmp snooping`
		`(config-if)# ip igmp snooping`

Table continues…

Issue number	Description	Workaround
	`BEB_1:1(config)#CP1 [06/26/13 05:01:58.985] 0x0006c69e 01b00001 DYNAMIC SET GlobalRouter IPMC ERROR The maximum number of Egress Records (pepstreams) 7901 has been reached!! CP2 [06/26/13 05:01:59.053] 0x0006c6a4 00000000 GlobalRouter IPMC ERROR ipmSysAllocEgressRec FAIL PepStrGetNew G 232.31.12.4 InVlanId 2412 CP1 [06/26/13 05:01:58.988] 0x0006c69f 01b00001 DYNAMIC CLEAR GlobalRouter IPMC ERROR The number of Egress Records (pepstreams) is now below the maximum number supported 7901`	
wi01117073	`ISIS WARNING isisCheckPtptSrm:send lsp 00be.b000.0200.00-43 seq112. invalid lsp (nil) or len 27` messages intermittently appear on the console when both IST peers booted simultaneously.	There is no functional impact observed.
wi01128615	When a VSP 9000 receives MinM packets with a Destination MAC as that of its own BMAC, ingress mirroring on NNI ports will show the B-TAG ethertype as 0x88A8 even if 0x8100 was used on the wire.	—
wi01177656	The counters for the **`show isis spbm drop-stats port unknown-unicast-sa`** command do not increment when used with a 9048XS-2 I/O module.	—
wi01181089	When making changes to route redistribution into ISIS while LSP usage is greater than 128, all routes may not be properly redistributed.	Disable redistribution of routes into ISIS until LSP usage falls below 128 LSP's, then re-enable and apply redistribution.
wi01188301	IS-IS "subnet allow" and "subnet suppress" are not supported.	—
wi01192838	IS-IS LSDB Host Name set to NULL before the LSPID life time expires.	—
wi01196147	A maximum of 20,000 routes are advertised per BEB.	—

Table continues…

Issue number	Description	Workaround
wi01201590	IS-IS routes can stop being redistributed while configuring IS-IS Accept Policies.	Apply the accept policies again.

Additional Known Issues

Issue Number	Description	Workaround
wi01181840	Remote fault recognition is not functioning correctly for 1G optics. The local switch will continue to attempt transmit data if transmit connection is broken.	—
wi1195104	Not all IPFIX flows are exported on the 9048XS-2 module.	—

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 19: Limitations and expected behaviors

Issue number	Description	Workaround
wi00511257	If you change the priority of, and then disable and enable the MLT port on an Ethernet Routing Switch 8600, the port takes 35 seconds to become the designated forwarding port on the root bridge. This condition causes traffic interruption for 35 seconds.	—
wi00511527	MSTP bridges may not learn the correct CIST regional root.	If you encounter this problem you can change the bridging priority of the switch to make sure the root selection occurs as desired.
wi00565499	If you use VSP and Ethernet Routing Switch 8600 on a VLAN, and all systems operate in MSTP mode, a loop can be generated if you restart a VLAN port on the Ethernet Routing Switch.	Disable the links on the Ethernet Routing Switch.
wi00664833	The MAC DA filter only applies for traffic that is bridged through the device. If the	Use ACL-based filters to implement the MAC DA filter. The ACL-based filter

Table continues…

Issue number	Description	Workaround
	packet is routed, then the legacy MAC DA filter does not apply for traffic that is routed through the box.	works correctly regardless of whether the packet is bridged or routed.
wi00689238	If a VSP 9000 aggregation switch sends a high volume (more than 3000) of OSPF or RIP routes to an Ethernet Routing Switch 8600 edge device to redistribute into an OSPF domain, the CPU utilization of the edge device can increase, which results in dropping all VLACP packets from the VSP device. The VLACP link operational state is down.	—
wi00691506	A topology change of an SMLT link between VSP 9000 systems and Ethernet Routing Switch 8600 Release 5.1.3 results in dropped packets. This problem occurs when one of the two MLT ports of the ERS is not a designated port or a root port. Topology changes make this port a blocking port and also other ports of the MLT change to the same state (blocking).	—
wi00732215	When all members of an LACP aggregation go down, the ARP record corresponding to the aggregation gets deleted and needs to be re-ARPed to forward traffic across IST.	To work around this problem use regular MLT interfaces instead of LACP interfaces. If LACP is required, the traffic recovery time will be between 1-12 seconds based on volume of re-ARPing required.
wi00733551	The Bandwidth Allocation Group (BAG) rate configuration of all ports is based on the maximum port speed of the module during the system bootup time. When you configure an interface shaper and it is lower than the maximum port speed, the BAG rate becomes larger than the port forwarding rate. This condition is an incorrect Qos configuration. As a result, low priority traffic is not dropped as expected.	—
wi00820028	You should clear the cache of the browser used to configure and monitor the device after an image upgrade. If this is not done incorrect screen displays can result.	Clearing the browser cache is found in **Tools** > **Internet Options** > **Browser History** > **Delete** > **Delete all ….** in Internet Explorer 7.0 and in **Tools** > **Clear Recent History** > **Select all options** > **Clear Now** in Firefox 3.6.x.

Table continues…

Issue number	Description	Workaround
wi00854206	For VLACP enabled links, recommended values exist for the configuration of the VLACP timers. However, in an SMLT topology, with VLACP and multicast both enabled on the SMLT link, you may need to adjust or increase the VLACP timers on that link to accommodate for a scaled multicast environment where there is a higher processing load on the CP, especially during failover events. This higher load can affect the ability to process VLACP keep-alive messages in a timely manner, which can cause the link to flap. You may need to configure timers proportionately to the anticipated multicast route load.	Avaya recommends that you configure IST links with a VLACP timeout of long, timeout scale of 3, and slow-periodic-time of 30 000 ms. These links are not impacted by multicast scaling considerations.
wi00981875	VSP 9000 management-plane-initiated applications that do not have VRF specific context are biased toward the Management Router routing table. When you configure a default route on both the Management Router and the Global Router, the default route on the Management Router takes precedence.	If you require both in-band management (Global Router) and out-of-band management (Management Router), the default route should not be present on the Management Router. Configure static routes for specific management networks in the desired VRF instead.
wi01068569	If you disable redistribution, and then apply a policy, you receive a warning that you need to apply the policy even though you already did. When you enable redistribution, and then apply the policy, you do not receive the warning because you already applied the policy. This is working as expected.	—
wi01086118	Ingress port mirroring does not work if the VLAN for the incoming packet does not match the VLAN for the port.	—
wi01162590	Do not enable LACP on IST ports.	Use MLT configuration with VLACP long timers. To remove an IST configuration, use the `no ist peer-ip` command. For more information about LACP configuration, see *Link Aggregation*

Table continues…

Issue number	Description	Workaround
		Control Protocol (LACP) 802.3ad and VLACP for VSP and ERS Technical Configuration Guide, NN48500-502.
wi01164112	If you disable LACP on a square or full-mesh core network because you need to make an LACP configuration change, you can cause a looping scenario.	If you need to modify the LACP configuration, for example, change the LACP key, on a square or full-mesh core network, you must perform the following tasks: 1. Shutdown all LACP ports. 2. Make the configuration change. 3. Bring all LACP ports back up.
wi01167121	You can experience loss of multicast and broadcast traffic if you mix interface speeds in the same VLAN and on the same slice. For example, ports 4/1, 3/1 and 3/2 are in the same VLAN. 3/1 is a 1 Gbps port and 3/2 is a 10 Gbps port. If 4/1 is sending broadcast or multicast traffic in the VLAN, the maximum output from 3/2 will be the same as 3/1. If 4/1 is sending 2 Gbps of traffic, 3/1 and 3/2 will have a maximum of 1 Gbps output. If the ports are on different slices, the 1 Gbps port will send 1 Gbps of traffic and the 10 Gbps port will send 2 Gbps of traffic. A slice is equal to two lanes. A lane refers to the following grouping of ports on an I/O module: • For 24-port modules: a group of four ports, for example 1-4 or 5-8, and so on. • For 48-port modules: a group of eight ports, for example, 1-8 or 9-16, and so on.	Do not mix interface speeds within the same group of ports that comprise a slice and are members of the same VLAN.

MLT configuration recommendation

MLT is designed for redundancy and robustness for when the components and subsystems that comprise the network fail. To take advantage of this, it is suggested that MLT links span different I/O cards so that if there is a failure on a card it only takes down one MLT link and the others continue to operate normally. If there are more MLT ports required on a single card, those links should reside in different slices on a given card. A slice is a grouping of ports that are handled by a single forwarding engine on the I/O card.

show pluggables Command

You may have to wait up to 30 seconds between subsequent `show pluggables` commands to give time for pluggable information to be refreshed.

Flash drive format

New external flash devices come with a FAT16 format. While this appears to work correctly when inserted into a 9080CP card, there is an incompatibility issue when there are more than 169 log files created. The incompatibility will cause the logging mechanism to stop writing any new log files. To correct this issue you need to reformat any new flash device after it has been inserted into the 9080CP with the `dos-format` command as explained in the document *CP Module Compact Flash Replacement*.

Power supply LEDs

VSP 9000 Power Supply LEDs are in a non-deterministic state when the CP Power Supply indicator is lit RED, indicating a fault. There will be log messages indicating the Power Supply fault event but the LEDs may be RED, GREEN or OFF.

IPFIX and IS-IS

IPFIX is not supported on IS-IS interfaces. Log messages such as the following will appear repeatedly in the log files:

```
IO3 [10/25/13 13:58:50.722] 0x0001c68d 00000000 GlobalRouter HW ERROR getSlotIdFromLpid:
LPID (2868) is not associated with a slot!
IO3 [10/25/13 14:02:30.791] 0x000005e0 00000000 GlobalRouter SW ERROR Invalid LPID: 2904
for getPimPortFromLpid conversion!!!
```

Displaying egress QoS queue weights

There is no mechanism to display the egress QoS queue weights in general or on a port basis.

The no ist enable command

The **`no ist enable command`** only dynamically disables an IST. It does not delete it. The IST will become enabled again the next time the chassis restarts.

Chapter 6: Resolved issues

This chapter identifies the issues resolved in Release 4.0.1.

Alarm, logging, and error reporting

Table 20: Resolved issues

Issue number	Issue description
wi00980601	Enabling tracing to log can affect system performance in scaled environments.
wi00986085	After a CP switch-over the following message can appear in the logs: `smltTick: Initial MAC/ARP tbl completed, unlocked SMLT/SLT ports.` The SMLT/SLT ports were not locked during the switch-over. This message is incorrectly reused in this situation.
wi01131833	The error message is incorrect when removing the 9012RC cooling module (rear cooling module); the system displays a warning message for the front 9012FC cooling module.

Chassis operations

Table 21: Resolved issues

Issue number	Issue description
wi01125186	If you configure a static route with less than 8 bit mask in the Mgmt VRF (Global Router VRF works fine), the standby CP will core if you try to perform a software upgrade of the chassis. If you try to enable, disable, or delete that static route then the primary CP will core.

Table continues…

Issue number	Issue description
wi01130024	The `show sys-info temp` command does not show Zone 2 for I/O modules. This component may be depopulated in future hardware releases. Further, as this is a cooler thermal point, it is not a driving factor in cooling the chassis as the warmest sensor on a blade determines fan speed.

COM

Table 22: Resolved issues

Issue number	Issue description
wi01130603	In COM, the EDM Plugins Inventory does not display the SVN Revision Number of the plugin.

EDM

Table 23: Resolved issues

Issue number	Issue description
wi01111210	A discrepancy exists between EDM and ACLI behavior when removing ports from ACL filters if the slot is down. You should not be able to remove the ports of a IO slot that is operationally down from the filters if the module is down. In EDM, you can remove the ports of such a slot, whereas ACLI does not allow to remove the same.
wi01127551	EDM/COM does not correctly display RSMLT status for IPv6. If you click on the **Configuration** > **VLAN** > **VLANs** > **IP** > **RSMLT** tab, the **Enable** checkbox appears cleared even though RSMLT shows as up and running through the ACLI. The ACLI shows the status correctly and in EDM/COM, going to **Configuration** > **IPv6** > **IPv6** > **Interfaces**- the **RsmltEnable** field displays the correct status for the VLAN.
wi01152214	Cannot access EDM using Firefox version 27.

HA operations

Table 24: Resolved issues

Issue number	Issue description
wi01201161	Issues have been observed with first generation I/O modules when PCAP is enabled and an HA failover occurs.

Management and general administration

Table 25: Resolved issues

Issue number	Issue description

wi01131449	The device can display the following messages when an invalid MIB GET request occurs for non-existent ports.
	`IO5  [09/05/13 03:30:48.655] 0x0011052a 00000000 GlobalRouter COP-SW ERROR lcdPimPortToMac: invalid PIM_PORT[63]`
	`IO5  [09/05/13 03:30:48.655] 0x0011052a 00000000 GlobalRouter COP-SW ERROR lcdPimPortToMacPort: invalid PIM_PORT[63]`
	`IO5  [09/05/13 03:30:48.655] 0x0025c554 00000000 GlobalRouter COP-SW ERROR cb_sw_port_get_stats error: wrong unit[4]`

wi01137524	If you configure the CP limit on slot/port 9/1, the device incorrectly configures the CP limit on management port 1/1, which causes an invalid configuration to load.

MLT, SMLT, and link aggregation

Table 26: Resolved issues

Issue number	Issue description
wi00822571	In rare occurrences traffic loops can be introduced if ports are removed from an MLT before being disabled.

Table continues…

Issue number	Issue description
wi01097311	If you have a configuration in which LACP and static MLT ports of an SMLT belong to the same lane, when the access ports are shut, the SMLT port mask of one of the static MLT ports is not updated correctly. The port mask indicates that the MLT port is up while it is actually down. Because the system thinks that the port is up, traffic is hashed onto it, which eventually is dropped because the port is down. A lane refers to the following grouping of ports on an I/O module: • For 24-port modules, such as 9024XL: a group of four ports, for example 1-4 or 5-8, and so on. • For 48-port modules, such as 9048GB or 9048GT: a group of eight ports, for example, 1-8 or 9-16, and so on.

Routing

Table 27: Resolved issues

Issue number	Issue description
wi01099098	You cannot use CFM between VSP 9000 and ERS 8800 to perform an l2 ping or l2 traceroute for a C-MAC.
wi01140262	BGP peer groups for VRFs are not saved correctly in the configuration file. The `ip bgp` statement is missing from the configuration file.
wi01141461	The IPv6 filtering functionally is not supported and should not be used even though the ACLI commands are visible. These commands will be removed in Release 3.4.1.
wi01145272	Virtual Router Redundancy Protocol (VRRP) not working on Network-to-Network Interface (NNI).
wi01198679	Previous to 3.4.0.0, enforcement of the Max DHCP Relay forwarders limit of 512 per VRF did not work. Upgrading from pre 3.4.0.0 to 3.4.x.x release where enforcement is applied will cause loss of any forwarders above the 512 limit. The system limit was and still is 1024 DHCP Relay forwarders per chassis.

SPBM and IS-IS

Table 28: Resolved issues

Issue number	Issue description
wi01151658	IS-IS adjacencies are brought down (deleted) before their hold-down time expire, which results in unnecessary flapping within the SPB network.
wi01117528	Abnormal shutdown seen when CFM C-MAC **`l2 traceroute <A.B.C.D>`** runs.
wi01137529	Newly created VLANs with VRFs and I-SIDs do not have the routing bit set.
wi01137534	SPBM Layer 2 Virtual Services Network (VSN) connectivity issue due to broadcast traffic, such as ARP requests, not being transmitted out of a MultiLink Trunking (MLT) port with Intermediate-System-to-Intermediate-System (IS-IS) enabled on it. You will only see the issue if you do not add ports to the MLT after you enable IS-IS on the MLT.
wi01137858	IS-IS IP route metric reset to one after route-policies are disabled.
wi01141033	A discovered I-SID may be labelled incorrectly as type local.

QoS and filters

Table 29: Resolved issues

Issue number	Issue description
wi01200839	When an egress port is oversubscribed, EF traffic is only allotted 10% regardless of the assigned QoS weighting.

Additional Resolved Issues

Issue Number	Description
wi01188236	Traffic to black hole routes sends to CP and overloads.

Table continues…

Issue Number	Description
wi01190660	If the flow is egressing on an MLT, we can only report the MLTid in the IPFIX export information, the MLT port resolution is not available.
wi01190598	If only one CP in Slot 2, the 9048XS—2 module will not boot up.
wi01190448	Do not use export or export-flush command for IPFIX.

wi01189529	After a CPU switchover, the following messages might be seen on the backup CPU, when the routing table is being synced over:
	`CP2 [09/18/14 07:38:05.038] 0x000b45ba`
	`00000000 GlobalRouter SW ERROR`
	`rtmChangeListSyncCallback: vrfId: 0`
	`received entry can't be located dst`
	`2.4.216.0/ 255.255.255.0 owner 2 num_hops`
	`= 1 cl_type type=2 cl mask =2048`
	The route may not be found in the RTM (routing table manager), therefore the route does not get added to the change list.

wi01189530	After a CPU switchover, the following messages might be seen on the backup CPU, when the routing table is being synced over:
	`CP2 [09/18/14 07:38:04.097] 0x000bc59a`
	`00000000 GlobalRouter RIP ERROR`
	`ripRouteSyncCallback: RipAddRoute() failed`
	CP2 [09/18/14 07:38:04.097] 0x0001079a 00000000
	GlobalRouter HW ERROR
	framework_process_entity_data: Application Sync
	failed for entity:0x20524950 representing
	Module RIP ,event:3/3 maxNumEvents:15`
	When this happens, the backup CPU is unable to add the RIP route to the RTM

wi01157421	If fabric statistics are enabled on a 2nd generation IO module interface, the fabric is not counting drop statistics for COS queue 7.
wi01188422	The user should follow the documented procedure to remove modules.
wi01188763	Resetting cards in parallel could cause issues.
wi01190429	When there are both static and dynamic IGMP receivers for the same group that point to an SMLT that has gone down and come back up, a timing issue can occur.

Table continues…

Issue Number	Description
wi01190905	The following sequence of commands will cause ports administratively enabled prior to the command execution to not be enabled after command execution: 1. **`slot shutdown <slot_number>`** 2. **`no sys power slot <slot_number>`** 3. **`sys power slot <slot_number>`** 4. **`no slot shutdown <slot_number>`**
wi01194014	Temperature, power, voltage, or bias threshold information may sometimes be reported incorrectly when a transceiver is already inserted in a port when a module starts up or newly inserted into a port. This does not cause any issues with the operation of the transceiver or the port.

Appendix A: Features and hardware models by release

This section provides an overview of the features and hardware models introduced in Releases 3.x and 4.0.

Features for Release 3.x and 4.0

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

Features	New in this release	
	4.0	3.x
Operations and Management		
Avaya CLI (ACLI) For more information, see *ACLI Commands Reference for Avaya Virtual Services Platform 9000,* NN46250-104.		X
Enterprise Device Manager (EDM) For more information, see *Using ACLI and EDM on Avaya Virtual Services Platform 9000,* NN46250-103.		X
File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) IPv4 addresses		X
File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) IPv6 addresses		X
Key Health Indicators (KHI) For more information, see *Monitoring Performance on Avaya Virtual Services Platform 9000,* NN46250-701.		X
Packet Capture Tool (PCAP) For more information, see *Troubleshooting Avaya Virtual Services Platform 9000,* NN46250-700.		X
SLA Mon™ For more information, see *Monitoring Performance on Avaya Virtual Services Platform 9000,* NN46250-701.		X
Simple Network Management Protocol (SNMP)		X

Table continues…

Features	New in this release	
	4.0	3.x
For more information, see *Configuring Security on Avaya Virtual Services Platform 9000,* NN46250-601.		
SSH and secure copy (SCP) For more information, see *Administering Avaya Virtual Services Platform 9000,* NN46250-600.		X
SSH client support For more information, see *Administering Avaya Virtual Services Platform 9000,* NN46250-600.		X
VSP Talk For more information, see *Administering Avaya Virtual Services Platform 9000,* NN46250-600.		X
Layer 2		
Bridge Protocol Data Unit (BPDU) Filtering For more information, see *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 9000,* NN46250-500.		X
IEEE 802.1D Mac Bridges/Spanning Tree IEEE 802.1w/s RSTP/MSTP IEEE 802.1p/Q Virtual LAN IEEE 802.3x Flow control (RX enabled/TX disabled) For more information, see *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 9000,* NN46250-500.		X
Layer 2 remote mirroring For more information, see *Troubleshooting Avaya Virtual Services Platform 9000,* NN46250-700.		X
Link Aggregation Control Protocol (LACP) and Virtual LACP (VLACP) For more information, see *Configuring Link Aggregation, MLT, and SMLT on Avaya Virtual Services Platform 9000,* NN46250-503.		X
Lossless Ethernet For more information, see *Network Design Reference for Avaya Virtual Services Platform 9000,* NN46250-200 and *Configuring Ethernet Modules on Avaya Virtual Services Platform 9000,* NN46250-508.	Not supported on second generation I/O modules.	X
Port, Source MAC, IP subnet, and Protocol-based VLANs For more information, see *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 9000,* NN46250-500.		X

Table continues…

Features	New in this release	
	4.0	**3.x**
MultiLink Trunking (MLT), Split MultiLink Trunking (SMLT) For more information, see *Configuring Link Aggregation, MLT, and SMLT on Avaya Virtual Services Platform 9000,* NN46250-503.		X
Simple Loop Prevention Protocol (SLPP) for more information, see *Administering Avaya Virtual Services Platform 9000,* NN46250-600.		X
Layer 3		
Address Resolution Protocol (ARP), Reverse ARP (RARP) For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 9000,* NN46250-505.		X
Border Gateway Protocol (BGP) For more information, see *Configuring BGP Services on Avaya Virtual Services Platform 9000,* NN46250-507.		X
BGP 4–byte AS For more information, see *Configuring BGP Services on Avaya Virtual Services Platform 9000,* NN46250-507.		X
Classless interdomain routing (CIDR) For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 9000,* NN46250-505.		X
Circuitless IP (CLIP) For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 9000,* NN46250-505.		X
Equal Cost Multipath (ECMP) For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 9000,* NN46250-505.		X
Internet Control Message Protocol (ICMP) For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 9000,* NN46250-505.		X
Internet Group Management Protocol (IGMP) For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 9000,* NN46250-504.		X
IGMP Layer 2 Querier For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 9000,* NN46250-504.		X

Table continues…

Features	New in this release	
	4.0	**3.x**
IGMP, virtualized For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 9000,* NN46250-504.		X
Internet Protocol Flow Information eXport (IPFIX) For more information, see *Monitoring Performance on Avaya Virtual Services Platform 9000,* NN46250-701.		X
IPv6 (OSPFv3, VRRP, RSMLT, and BGP+) For more information see *Configuring BGP Services on Avaya Virtual Services Platform 9000,* NN46250-507 and *Configuring IPv6 Routing on Avaya Virtual Services Platform 9000,* NN46250-509.	Not supported	X
Layer 3 remote mirroring For more information, see *Troubleshooting Avaya Virtual Services Platform 9000,* NN46250-700.		X
Open Shortest Path First (OSPF) For more information, see *Configuring OSPF and RIP on Avaya Virtual Services Platform 9000,* NN46250-506.		X
Protocol Independent Multicast–Sparse Mode (PIM-SM), PIM-Source Specific Mode (PIM-SSM) For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 9000,* NN46250-504.		X
Routed Split MultiLink Trunking (RSMLT) For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 9000,* NN46250-505.		X
Routing Information Protocol (RIP) For more information, see *Configuring OSPF and RIP on Avaya Virtual Services Platform 9000,* NN46250-506.		X
Virtual Router Redundancy Protocol (VRRP) For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 9000,* NN46250-505.		X
Virtual Routing and Forwarding (VRF) For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 9000,* NN46250-505.		X
Upper layers		
Extensible Authentication Protocol over LAN (EAPoL)		X

Table continues…

Features	New in this release	
	4.0	3.x
For more information, see*Configuring Security on Avaya Virtual Services Platform 9000,* NN46250-601.		
Dynamic Host Configuration Protocol (DHCP) Relay For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 9000,* NN46250-505.		X
DHCP Relay Option 82 For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 9000,* NN46250-505.		X
Domain Name Service (DNS) For more information, see *Administering Avaya Virtual Services Platform 9000,* NN46250-600.		X
Microsoft Network Load Balancing (NLB) For more information, see *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 9000,* NN46250-500.		X
Microsoft NLB ARP multicast-MAC-flooding support For more information, see *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 9000,* NN46250-500.		X
Network Time Protocol (NTP) For more information, see *Administering Avaya Virtual Services Platform 9000,* NN46250-600.		X
Remote Access Dial-In User Services (RADIUS) IPv4 For more information see, *Configuring Security on Avaya Virtual Services Platform 9000,* NN46250-601.		X
RADIUS IPv6 For more information see, *Configuring Security on Avaya Virtual Services Platform 9000,* NN46250-601.	Not supported	X
Terminal Access Controller Access Control System Plus (TACACS+) For more information, see *Configuring Security on Avaya Virtual Services Platform 9000,* NN46250-601.		X
User Datagram Protocol (UDP) For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 9000,* NN46250-505.		X
Avaya VENA Fabric Connect		
Connectivity Fault Management (CFM)		X

Table continues…

Features	New in this release	
	4.0	3.x
For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 9000,* NN46250-510.		
IS-IS accept policies, see IS-IS accept policies on page 16.	X	
IS-IS adjacencies scaling Release 4.0 offers enhanced scaling for IS-IS adjacencies. Support increases to 128 adjacencies, up from 64 in prior releases.	X	
Shortest Path Bridging MAC For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 9000,* NN46250-510.		X
Multicast over Shortest Path Bridging MAC For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 9000,* NN46250-510.		X
Quality of Service and filtering		
Diffserv framework For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 9000,* NN46250-502.		X
Quality of Service (QoS) For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 9000,* NN46250-502.		X
Traffic filtering For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 9000,* NN46250-502.		X

Hardware models for Release 3.x and 4.0

The following table provides a list of the hardware models and components introduced in Releases 3.x and 4.0

Model or component	Part number	Release
Chassis		
Virtual Services Platform 9010 AC chassis, see *Installing the Avaya Virtual Services Platform 9000,* NN46250-304.	EC1402002-E6	3.4

Table continues…

Model or component	**Part number**	**Release**
Virtual Services Platform 9012 chassis, see *Installing the Avaya Virtual Services Platform 9000,* NN46250-304.	EC1402001- E6	3.0
Control Processor module		
9080CP Control Processor module, see *Installing Modules in Avaya Virtual Services Platform 9000,* NN46250-301.	EC1404007-E6	3.0
Cooling modules		
9012FCHS high-speed cooling module, see *Installing Cooling Modules in Avaya Virtual Services Platform 9000,* NN46250-302.	EC1411004 –E6	3.4.3
9010CM cooling module, see *Installing Cooling Modules in Avaya Virtual Services Platform 9000,* NN46250-302.	EC1411012-E6	3.4
9012RC Switch Fabric cooling module, see *Installing Cooling Modules in Avaya Virtual Services Platform 9000,* NN46250-302.	EC1411002- E6	3.0
9012FC IO cooling module, see *Installing Cooling Modules in Avaya Virtual Services Platform 9000,* NN46250-302.	EC1411001- E6	3.0
Input/Output modules		
9048XS-2, see 9048XS-2 I/O module on page 19.	EC1404005-E6	4.0
9012QQ-2, see 9012QQ-2 I/O module on page 19.	EC1404008-E6	4.0.1
9024XL, see *Installing Modules in Avaya Virtual Services Platform 9000,* NN46250-301.	EC1404001-E6	3.0
9048GB, see *Installing Modules in Avaya Virtual Services Platform 9000,* NN46250-301.	EC1404002-E6	3.0
9048GT, see *Installing Modules in Avaya Virtual Services Platform 9000,* NN46250-301.	EC1404003-E6	3.0
Power supply		
9006AC power supply, see *Installing AC Power Supplies in Avaya Virtual Services Platform 9000,* NN46250-303.	EC1405A01-E6	3.0
Switch Fabric module		
9095SF module, see *Installing Modules in Avaya Virtual Services Platform 9000,* NN46250-301.	EC1404009-E6	3.4
9090SF Switch Fabric module, see *Installing Modules in Avaya Virtual Services Platform 9000,* NN46250-301.	EC1404006- E6	3.0