



Release Notes — Release 3.4.0.2

Avaya Virtual Services Platform 9000

Release 3.4.0.2
NN46250-401
Issue 05.05
February 2014

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "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.

License types

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

Heritage Nortel Software

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

Copyright

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

Third Party Components

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

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a

corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction	9
Purpose.....	9
Related resources.....	9
Documentation.....	9
Training.....	9
Avaya Mentor videos.....	10
Subscribing to e-notifications.....	10
Support.....	12
Searching a documentation collection.....	12
Chapter 2: New in this release	15
Features.....	15
Other changes.....	16
Chapter 3: Important notices and new features	19
New features.....	19
New hardware supported in Release 3.4.....	24
Virtual Services Platform 9010 AC chassis.....	24
9095SF module.....	31
9010CM cooling module.....	32
Existing hardware supported in the current release.....	32
Virtual Services Platform 9012 chassis.....	32
9006AC power supply.....	33
9012FC cooling module.....	33
9012RC cooling module.....	33
9024XL interface module.....	34
9048GB interface module.....	39
9048GT interface module.....	41
9080CP Control Processor module.....	41
9090SF Switch Fabric module.....	43
Removing a master CP module with CPU-HA mode activated.....	44
Removing external storage devices from the CP module.....	44
File names for this release.....	46
Important information and restrictions.....	47
Protecting modules.....	48
Resetting multiple modules.....	49
Supported browsers.....	49
Environmental specifications.....	49
Reliability.....	51
IPv4 interface MTU.....	52
Supported system and management applications with IPv6.....	52
User configurable SSL certificates.....	53
EDM image management.....	53
Feature licensing.....	53
Fixes from previous releases.....	54
Hardware and software compatibility.....	54

Other documents.....	59
Chapter 4: Software and hardware scaling capabilities.....	61
Hardware scaling capabilities.....	61
Software scaling capabilities.....	62
Chapter 5: Supported standards, request for comments, and Management Information Bases.....	67
Supported standards.....	67
Supported RFCs.....	68
Quality of service.....	71
Network management.....	72
MIBs.....	73
Standard MIBs.....	75
Proprietary MIBs.....	78
Chapter 6: Known issues and limitations.....	79
Known issues.....	79
Alarm, logging, and error reporting.....	79
Applications.....	81
Chassis operations.....	82
COM.....	84
EDM.....	85
HA operations.....	86
Hardware.....	87
Management and general administration.....	88
MLT, SMLT, and link aggregation.....	90
Multicast.....	91
Patching and upgrading.....	92
Routing.....	93
SPBM and IS-IS.....	96
Interoperability issues.....	98
Limitations.....	99
Chapter 7: Resolved issues in Release 3.4.0.2, Release 3.4.0.1, and Release 3.4.0.0..	103
Resolved issues in Release 3.4.0.2.....	103
Application connectivity issue.....	103
Failed RSP Microcode ERROR.....	104
IP redirect next-hop filter.....	104
High Availability with CFM C-MAC.....	104
Resolved issues in Release 3.4.0.1.....	104
Routing.....	104
Resolved issues in Release 3.4.0.0.....	105
Alarm, logging, and error reporting.....	105
Applications.....	105
COM.....	106
EDM.....	106
Hardware.....	107
Management and general administration.....	107
Patching and upgrading.....	108
Routing.....	109

SPBM and IS-IS.....	109
VLAN operations.....	110

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 *Avaya Virtual Services Platform 9000 Documentation Roadmap*, 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

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.

- To find videos on the Avaya Support website, go to <http://support.avaya.com>, select the product name, and check the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to <http://www.youtube.com/AvayaMentor> and perform one of the following actions:
 - Enter a key word or key words in the Search Channel to search for a specific product or topic.
 - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

 **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 web site.

About this task

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

Procedure

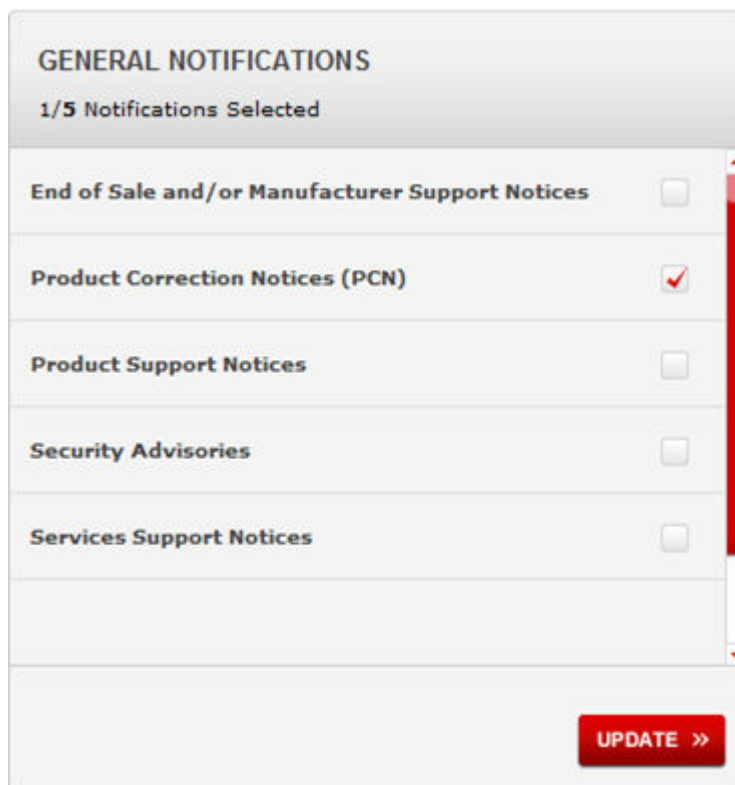
1. In an Internet browser, go to <https://support.avaya.com>
2. Type your username and password, and then click **LOG IN**.
3. Click **MY PROFILE**.



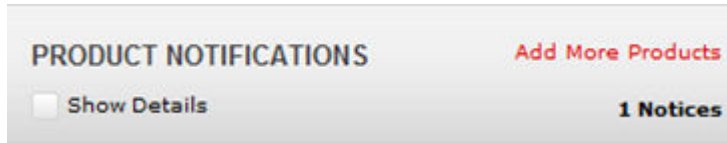
4. On the site toolbar, click your name, and then select **E Notifications**.



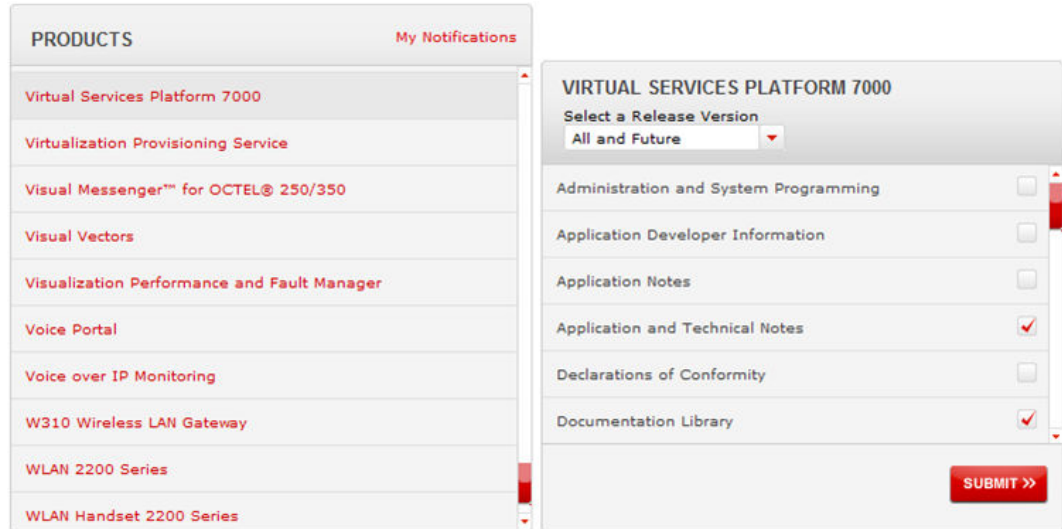
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.



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



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



11. Click **Submit**.

Support

Visit the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

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 *Avaya Virtual Services Platform 9000 Release Notes* (NN46250–401) for Release 3.4.0.0, 3.4.0.1, and 3.4.0.2.

Features

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

New feature support

Release 3.4.0.2 adds the following new software features:

- ACLI enhancements
- Bridge Protocol Data Unit (BPDU) Filtering
- Connectivity Fault Management (CFM) enhancements
- Enterprise Device Manager (EDM) copy and paste
- EDM Help file enhancement
- HTTPS port configuration
- Internet Group Management Protocol (IGMP) Layer 2 querier
- IGMP virtualization
- IP multicast over Shortest Path Bridging MAC (SPBM)
- IPv6 traceroute
- Ping
- Route map
- SLA Monitor
- SNMP server
- SPBM packet drop statistics
- Terminal Access Controller Access Control System Plus (TACACS+)
- Traffic filtering update

For more information, see [New features](#) on page 19, [Software and hardware scaling capabilities](#) on page 61, and [Supported standards, request for comments, and Management Information Bases](#) on page 67.

New hardware support

Release 3.4.0.2 adds support for a 1000BASE-T SFP on the 9024XL module and adds support for a 10GBASE-ZR SFP+. For the list of SFPs and SFP+s that the 9024XL module supports, see [9024XL interface module](#) on page 34.

Release 3.4.0.2 adds support for the following new hardware:

- Virtual Services Platform 9010 AC chassis
- 9095SF module
- 9010CM cooling module

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

- [New hardware supported in Release 3.4](#) on page 24
- [Using the VSP 9024XL Ventilation Cover for VSP 9010](#) on page 38
- [Environmental specifications](#) on page 49
- [Reliability](#) on page 51
- [Hardware and software compatibility](#) on page 54
- [Hardware scaling capabilities](#) on page 61

Release 3.4.0.2 qualified support for new CWDM SFP+ devices. [9024XL interface module](#) on page 34 and [Hardware and software compatibility](#) on page 54 are updated to include these devices.

Other changes

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

New Introduction chapter

The Introduction chapter replaces the Purpose of this document and Customer service chapters.

Browser support for EDM

[Supported browsers](#) on page 49 is updated.

IPv4 interface MTU

[IPv4 interface MTU](#) on page 52 is added to the document.

Known issues

[Known issues](#) on page 79 is updated.

Resolved issues

[Resolved issues in Release 3.4.0.2, Release 3.4.0.1, and Release 3.4.0.0](#) on page 103 is updated for issues fixed in Release 3.4.0.2, 3.4.0.1 and 3.4.0.0.

Upgrading Avaya Virtual Services Platform 9010

For Avaya Virtual Services Platform 9010, Avaya supports the following two upgrade paths for Release 3.4:

- Release 3.2.x to Release 3.4. To follow this upgrade path, you must contact Avaya Support through <http://support.avaya.com>.
- Release 3.3.3.0 and later to Release 3.4.

You do not need to upgrade through all of the intermediate releases. For Avaya Virtual Services Platform 9010, choose an upgrade path from Release 3.2.x to Release 3.4, or from Release 3.3.3.x to Release 3.4.

For more information, see

- [Virtual Services Platform 9010 AC chassis](#) on page 24.
- [Upgrading from Release 3.3.3.0 or later to Release 3.4](#) on page 25.

New in this release

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.

New features

This section highlights the feature support added in Release 3.4.

ACLI enhancements

Release 3.4 makes enhancements to Avaya Command Line Interface (ACLI). The following list describes these enhancements:

- The **show software** command adds an optional verbose parameter. The output for the **show software verbose** command includes a date and time stamp to indicate when you last added, activated, and committed a software release. The output also indicates if you manually committed the software release, or if you used the automatic commit feature. For more information, see *Avaya Virtual Services Platform 9000 Upgrades and Patches — Software Release 3.4*, NN46250–400.

If you downgrade to a release prior to Release 3.4, the system displays the following error message:

```
Unable to update release information for release <release name>
```

You can ignore the error message; it has no functional impact. 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.

- You can use the **show history** command to view a list of previously run commands. You can run one of the commands again by using the **!(command number)** command. See the following text for an example of how to use these commands:

```
VSP-9012:1(config)#show history
1 en
2 con t
3 show history
4 show mlt
5 show lacp interface mlt
6 show vlan advance 2
7 show history
```

```
VSP-9012:1(config)#!4  
VSP-9012:1(config)#show mlt
```

- You can use the **software reset-commit-time** [<1-60>] command to extend or reduce the commit time after you apply a software upgrade or patch. You may need additional time to verify the software works as expected after the upgrade or patch before you commit or roll back.

For more information about these commands, see *Avaya Virtual Services Platform 9000 Commands Reference — CLI*, NN46250–104.

- All user-access levels can use the **Telnet** command to gain access to another device.
- You can use new commands to show and delete debug files, for example, core files or archive files. For more information, see *Avaya Virtual Services Platform 9000 Troubleshooting*, NN46250–700.

BPDU Filtering

Use BPDU Filtering to achieve the following results:

- Block the root selection process after an edge device, such as a laptop that uses Linux with STP enabled, is added to the network. Blocking the root selection process prevents unknown devices from influencing the spanning tree topology.
- Block BPDU flooding of the switch from an unknown device.

For more information about how to configure BPDU Filtering, see *Avaya Virtual Services Platform 9000 Configuration — VLANs and Spanning Tree*, NN46250–500.

CFM enhancements

Release 3.4 enhances Connectivity Fault Management (CFM) support to make it easier to configure CFM for Shortest Path Bridging MAC (SPBM). Instead of configuring explicit Maintenance End Points (MEP) and Maintenance Intermediate Points (MIP), and then associating multiple VLANs with the MEPs and MIPs, you can now use auto-generated CFM commands that create a MEP and MIP at a specified level for every SPBM Backbone VLAN (B-VLAN) or customer VLAN (C-VLAN) on the chassis.

Except for C-VLANs, you have a choice to still configure explicit MEPs and MIPs, or you can use the new auto-generated commands. For C-VLANs, you can configure only one MEP or MIP for each C-VLAN and you must use the auto-generated commands.

Another major enhancement is that CFM extends the debugging of Layer 2 networks. In Release 3.3, you could debug the SPBM B-VLANs only. Now you can debug the C-VLANs as well. Use this enhancement to isolate a connectivity fault in either the SPBM cloud or in a customer domain. CFM breaks the network into sections so you can determine exactly where the problem exists.

For more information on how to configure or use the CFM enhancements, see *Avaya Virtual Services Platform 9000 Configuration — Shortest Path Bridging MAC (SPBM)*, NN46250–510.

Enterprise Device Manager copy and paste

Beginning with Release 3.4, you can copy and paste data for the following scenarios:

- From one cell to one or more cells on the same EDM tab
- From one cell to one or more cells across multiple EDM tabs
- From EDM to the clipboard outside the web browser

EDM cells must be editable and use the same data type. For more information, see *Avaya Virtual Services Platform 9000 User Interface Fundamentals*, NN46250–103.

EDM Help file enhancement

Prior to Release 3.4, EDM Help files had to be installed on a TFTP or FTP server. Release 3.4 still supports the TFTP and FTP server option but you can also store the Help files locally using either the internal Compact Flash, the external Compact Flash, or a USB storage device on the 9080CP module. For more information about how to configure EDM to use the Help files, see *Avaya Virtual Services Platform 9000 User Interface Fundamentals*, NN46250-103.

HTTPS port configuration

In previous releases, the HTTPS port assignment was fixed at 443. Beginning with Release 3.4, you can change that default port assignment. For more information, see *Avaya Virtual Services Platform 9000 User Interface Fundamentals*, NN46250–103.

Important:

Discover the ports that UDP and TCP already use before you select a port for HTTPS. Use the `show ip tcp connections` command to list the ports already in use, and then select a port that does not appear in the command output.

Avoid using ports 1024 to 1100.

IGMP Layer 2 querier

Release 3.4 introduces the Internet Group Management Protocol (IGMP) Layer 2 Querier feature. You can use this feature to provide a querier on a Layer 2 network without a multicast router. For more information see *Avaya Virtual Services Platform 9000 Configuration — IP Multicast Routing Protocols*, NN46250–504.

IGMP virtualization

Beginning with Release 3.4, Virtual Services Platform 9000 adds multicast support for the Virtual Routing and Forwarding (VRF) Lite feature. You can use VRF Lite to emulate many virtual routers with one router. Multicast virtualization includes:

- IGMP snooping
- IGMP in Layer 2 virtual services networks (VSN)
- IGMP in Layer 3 VSNs

For more information, see *Avaya Virtual Services Platform 9000 Configuration — IP Multicast Routing Protocols*, NN46250–504.

IP multicast over SPBM

Release 3.4 extends the SPBM Intermediate System to Intermediate System (IS-IS) control plane to exchange IP multicast stream advertisement and membership information. You can

now use SPBM for Layer 2 virtualization as well as Layer 3 routing and forwarding virtualization.

Virtual Services Platform 9000 supports three operational models for IP multicast over SPBM:

- Layer 2 VSN with IGMP support on the access network for optimized forwarding of IP multicast traffic in a bridge network (Layer 2 VSN with multicast)
- IP multicast routing support for the Global Routing table using SPBM in the core and IGMP on the access (IP Shortcuts with multicast)
- Layer 3 VSN with VRF-based IP multicast routing support over SPBM in the core and IGMP on the access (Layer 3 VSN with multicast)

Virtual Services Platform 9000 does not support NLB-multicast and NLB-multicast with IGMP for SPBM.

For more information about how to configure IP multicast over SPBM, see *Avaya Virtual Services Platform 9000 Configuration — Shortest Path Bridging MAC (SPBM)*, NN46250–510.

IPv6 traceroute

The `traceroute` command now supports IPv6 addresses. For more information, see *Avaya Virtual Services Platform 9000 Troubleshooting*, NN46250–700.

Ping

An enhancement to the ping command provides the ability to specify an outgoing interface as either an Ethernet port, vlan-id, out-of-band mgmt interface, or tunnel id.

For more information, see *Avaya Virtual Services Platform 9000 Commands Reference — CLI*, NN46250–104.

Route map

The syntax for IP route policy to ignore the route in Route-Map Configuration mode has changed. You can now configure the policy action to `[no] permit` within the policy sequence context. It was previously configured on policy sequence creation.

For more information about IP route policy, see *Avaya Virtual Services Platform 9000 Configuration — IP Routing*, NN46250–505.

SLA Monitor

Release 3.4 adds support for the Service Level Agreement (SLA) Monitor agent. Use the agent with an SLA Monitor server to analyze and monitor the network, based on application use and traffic flow. For more information about the agent, see *Avaya Virtual Services Platform 9000 Performance Management*, NN46250–701.

SNMP server

You can now use the `no snmp-server community-by-index <community index>` command to delete an SNMP community string by its index name. This command is in addition to the existing `no snmp-server community WORD<1-32>` command to delete the SNMP community by community string.

For more information, see *Avaya Virtual Services Platform 9000 Commands Reference — CLI*, NN46250–104.

SPBM packet drop statistics

Release 3.4 greatly enhances the way that packet drop statistics are reported to help system administrators identify problems in an SPBM network. Instead of simply counting the number of dropped packets per port, this feature provides more visibility into what traffic SPBM drops at NNI interfaces, and why. For more information, see *Avaya Virtual Services Platform 9000 Configuration — Shortest Path Bridging MAC (SPBM)*, NN46250–510.

TACACS+

Release 3.4 introduces support for Terminal Access Controller Access Control System Plus (TACACS+). Use TACACS+ to provide centralized user authentication, authorization, and accounting for router or network access server (NAS) access. For more information see, *Avaya Virtual Services Platform 9000 Security*, NN46250–601.

Traffic filtering

In Release 3.4, the mask operator used in traffic filtering for MAC addresses and IP addresses is updated. The mask operator is used to mask bits in packet fields during a search or to match on a partial value of a packet field.

The ACL and ACE configuration syntax for a mask is similar to how you use the equal operator except that you must provide the mask value. As part of the configuration you can specify a mask value (number) to represent the bits to mask in the attribute. If you use a decimal number for the mask, the mask value applies to the least significant bits on that attribute.

In Release 3.4, the update means that a mask of 24 used with an IP address is the same as a mask of 0.255.255.255, and a mask of 24 used with a MAC address is the same as 0x000000ffffff. A mask of 16 used with an IP address is the same as a mask of 0.0.255.255, and a mask of 32 used with a MAC address is the same as 0x0000ffffff.

The update changes the output for the `show filter acl config` command.

The mask parameter is also updated for the following commands:

- `filter acl ace ethernet <1-2048> <1-2000> <dst-mac|src-mac> mask WORD<1-1024> WORD<1-1024>`

Rule	Result
<pre>filter acl ace ethernet 10 10 dst- mac mask 0x01:00:5e:00:00:01 24</pre> <p>which is the same as</p> <pre>filter acl ace ethernet 10 10 dst- mac mask 01:00:5e:00:00:01 0x000000ffffff</pre>	<p>The rule matches only on the most significant 24 bits as they are not masked, for example, 01:00:5e, and does not care about the least significant 24 bits because they are masked; the least significant 24 bits can have a value of 00:00:00 - FF:FF:FF.</p>

- `filter acl ace ip <1-2048> <1-2000> <dst-mac|src-mac> mask WORD<1-1024> {<0-32|null|<A.B.C.D>}`

Rule	Result
<pre>filter acl ace ip 10 10 src-ip mask 2.10.10.12 24</pre>	<p>The rule matches only the most significant 8 bits, for example, 2, and does not care about the value of the remaining 24 bits because they are masked, for example, 10.10.12. Packets with a source IP address of 2.15.16.122 or 2.3.4.5 match on the filter rule while packets with a source IP address of 3.10.10.12 and 4.10.10.12 do not match on the filter rule. The mask appears as 0.255.255.255 in the command output for show filter acl config.</p>
<p>which is the same as</p> <pre>filter acl ace ip 10 10 src-ip mask 2.10.10.12 0.255.255.255</pre>	

For more information, see *Avaya Virtual Services Platform 9000 Configuration — QoS and ACL-Based Traffic Filtering*, NN46250–502.

New hardware supported in Release 3.4

This section identifies the new hardware that Release 3.4 supports.

Virtual Services Platform 9010 AC chassis

The front of the Virtual Services Platform 9010 AC chassis provides two vertical slots for Control Processor (CP) modules and eight vertical slots for interface modules. The back of the chassis provides six horizontal slots for Switch Fabric (SF) modules. The chassis provides one additional slot below the SF modules for manufacturing use.

The airflow for cooling flows from front to back. Install two 9010CM cooling modules at the front of the chassis, below the CP and interface modules. The cooling modules cool the modules at the front of the chassis as well as the SF modules at the back.

You can install up to eight AC power supplies at the bottom front of the chassis. Ensure the power supplies are the same. The chassis does not support a mixed configuration of power supplies.

The following table provides the weight and dimensions of the Virtual Services Platform 9010 AC chassis.

Table 1: Virtual Services Platform 9010 AC chassis dimensions and weight

Width	17.19 in. (436.6 mm)
Height	36.1 in. (915 mm)

Depth	33.75 in. (857.85 mm)
Weight (chassis and midplane)	141 lb (64 kg)
Weight (chassis, midplane, and cooling modules)	181 lb (82 kg)

! Important:

COM support for Virtual Services Platform 9010 will be available in COM Release 3.1.

The CP modules in the Virtual Services Platform 9010 AC chassis must use a minimum software version of Release 3.4.

Avaya supports the following two upgrade paths for Release 3.4 on the Virtual Services Platform 9010 AC:

- Release 3.2.x to Release 3.4 — to follow this upgrade path, you must contact Avaya Support through <http://support.avaya.com>.
- Release 3.3.3.0 and later to Release 3.4 — to follow this upgrade path, follow the steps in [Upgrading from Release 3.3.3.0 or later to Release 3.4](#) on page 25.

*** Note:**

You do not need to upgrade through all of the intermediate releases. For Avaya Virtual Services Platform 9010, choose an upgrade path from Release 3.2.x to Release 3.4, or from Release 3.3.3.x to Release 3.4.

Upgrading from Release 3.3.3.0 or later to Release 3.4

Use the following procedure to upgrade the Avaya Virtual Services Platform 9010 from Release 3.3.3.0 or later to Release 3.4.

*** Note:**

If you are upgrading a Virtual Services Platform 9012, no restrictions exist for the upgrade. For a Virtual Services Platform 9012, you do not need to perform this interim upgrade from Release 3.3.3.0 or later to Release 3.4. You can skip this procedure and upgrade directly to Release 3.4.

Before you begin

- If you view the front of the Virtual Services Platform 9000 chassis, the Online LED for the CP module flashes green. This LED action indicates the chassis is ready for upgrade.
- The CP module in the chassis must be running Release 3.3.3.0 or later.
- If your system is a dual CP configuration, remove the CP module in slot 2.
- Using a network computer, download the VSP9K.3.4.0.0.tgz file and copy it to an external storage device that the CP module supports, such as USB or Compact Flash.

You can download the software from <http://support.avaya.com/downloads/>.

- Ensure the external storage device has at least 150 MB of free space to store the archived software.

If you need to backup the contents of an external Compact Flash device in a Virtual Services Platform 9000 system before you can delete the content and make space available, *Avaya Virtual Services Platform 9000 Administration*, NN46250–600 includes a procedure that shows how to backup and restore the contents of an external Compact Flash to USB.

- You must have a terminal or portable computer with a serial port and terminal-emulation software.
- You must have an Underwriters Laboratories (UL)-listed straight-through or null modem RS-232 cable with a female DB-9 connector for the console port on the CP module.

Procedure

1. Connect the serial port on the terminal to the console port on the master CP module in the chassis.

Ensure that you shield the cable that connects to the console port to comply with emissions regulations and requirements.

2. Turn on the terminal.
3. Insert the external storage device, either USB or Compact Flash, in to the CP module in slot 1.
4. Apply power to the chassis.

The system displays the following error, followed by the SW recovery menu:

```
CP1 [08/30/13 07:20:28.507] 0x00010832 00000000 GlobalRouter HW ERROR
This chassis type 40FE2300 is not compatible with this SW. Please refer to
any technical bulletins that came with this chassis for possible
directions on how to upgrade your SW, and/or contact your technical
support.
```

```
*****
* WARNING:
* We have detected that the software running on this CP module is
* not supported on this chassis. You need to install and/or select
* a supported version. Please consult the documentation that came
* with your hardware or contact Avaya Technical Support.
*****
```

```
Lifecycle SW recovery menu
```

```
1 - Add software release from removable device
2 - Select software release; Reboot
3 - Remove a software release
```

```
q - Quit/Reboot
```

```
Please make your selection:
```

5. Enter **1** to select the software release.

The system displays the following message:

```
Select media to scan for release archives
```

```

1 - /extflash
2 - /usb
Q - Quit

```

Please make your selection:

6. Enter **1** to select the external Compact Flash or **2** to select USB.
The system displays a list of all images on the device.

```
Select archive to add
```

```
1 - VSP9K.3.4.0.0.tgz
```

Please make your selection:

7. Enter the number that corresponds to the VSP9K.3.4.0.0.tgz archive.
The system extracts the image and stores it in the `/intflash/release/` directory on the CP module.

```
Extracting distribution information from VSP9K.3.4.0.0.tgz
Extracting release 3.4.0.0.GA from /usb/VSP9K.3.4.0.0.tgz
```

```
Lifecycle SW recovery menu
```

```
1 - Add software release from removable device
2 - Select software release; Reboot
3 - Remove a software release
```

```
q - Quit/Reboot
```

Please make your selection:

*** Note:**

If the internal flash does not have enough space to store the new image, you can use the SW recovery menu item 3 to remove existing software releases from the internal flash.

8. Enter **2** to select the software release.
The system displays a list of release choices:

```

*****
*                                                                 *
*  WARNING:                                                       *
*  If the chassis has dual CP modules this recovery option could  *
*  cause the CP modules to boot with different software versions  *
*  and potentially will get into boot loop situation. Please remove *
*  one CP before proceeding.                                       *
*                                                                 *
*****
1 - 3.4.0.0.GA
2 - 3.3.3.0.GA (Primary Release)

q - Quit

Please make your selection:

```

9. Enter the number that corresponds to the 3.4.0.0.GA release.
The CP module reboots with the new image. All other modules are upgraded, and then reboot again. Allow at least 15 minutes for the system to respond and provide

the login prompt. During the upgrade process, do not remove modules from the chassis.

10. Log in to CLI:

```
Copyright(c) 2010-2013 Avaya, Inc.
All Rights Reserved.
Virtual Services Platform 9000
Software Release Build 3.4.0.0
General Availability Released Software, Fully supported

AVAYA COMMAND LINE INTERFACE

CP1 [08/30/13 07:29:41.665] 0x00010757 00000000 GlobalRouter HW INFO
Initial configuration download to all cards completed
CP1 [08/30/13 07:29:41.666] 0x0003458b 00000000 GlobalRouter SW INFO The
system is ready
CP1 [08/30/13 07:29:41.666] 0x00004595 00000000 GlobalRouter SNMP INFO
Booted with file
Login: CP1 [08/30/13 07:29:43.265] 0x0000467d 00000000 GlobalRouter SNMP
INFO Power Supply Up(PsId=3, OperStatus=3)
CP1 [08/30/13 07:29:43.266] 0x0000467d 00000000 GlobalRouter SNMP INFO
Power Supply Up(PsId=4, OperStatus=3)
CP1 [08/30/13 07:29:43.266] 0x0000467d 00000000 GlobalRouter SNMP INFO
Power Supply Up(PsId=7, OperStatus=3)
CP1 [08/30/13 07:29:43.267] 0x0000467d 00000000 GlobalRouter SNMP INFO
Power Supply Up(PsId=8, OperStatus=3)
CP1 [08/30/13 07:30:29.781] 0x000045e5 00400005 DYNAMIC SET GlobalRouter
SNMP INFO Sending Cold-Start Trap
CP1 [08/30/13 07:30:29.783] 0x000005a7 00000006.1 DYNAMIC SET
GlobalRouter SW WARNING No configured hosts are reachable for log file
transfer
CP1 [08/30/13 07:31:41.658] 0x00088524 00000000 GlobalRouter SW INFO Boot
sequence successful
Login: rwa
Password: ***
You are currently running a new version of code.
This release will be auto-committed in 6 minutes and 36 seconds.
Version Running: 3.4.0.0.GA
CP1 [08/30/13 07:33:06.541] 0x000305ca 00000000 GlobalRouter SW INFO user
rwa connected via console port
```

11. Enter Privileged Exec mode:

```
VSP-9010:1>enable
```

12. Commit the software:

```
VSP-9010:1#software commit
Executing software commit for version 3.4.0.0.GA.
Software commit successful
```

13. If your system uses a dual-CP configuration, install the secondary CP module. The secondary CP module synchronizes the image with the master CP, and then reboots. Allow at least five minutes for the CP module to initialize after the reboot.

14. Stop the USB device:

```
VSP-9010:1#usb-stop
It is now safe to remove the USB device.
```

If you use an external Compact Flash to transfer the software files, you can skip this step.

15. Remove the USB device.

If you use an external Compact Flash to transfer the software files, do not remove the Compact Flash device from the CP module. Avaya recommends that you operate the chassis with an external Compact Flash installed.

16. Use the **show sys software** and **show software** commands to verify the upgrade was successful:

```
VSP-9010:1#show sys software
System Software Info :

Default Runtime Config File : /intflash/config.cfg
Config File :
Last Runtime Config Save : 0
Last Runtime Config Save to Slave : 0

Boot Config Table
Version : 3.4.0.0.GA on Friday Aug 30 07:26:22 EDT 2013
SlaveCpImageSyncState : N/A
PrimaryConfigSource : /intflash/config.cfg
SecondaryConfigSource : /intflash/config.cfg
EnableFactoryDefaults : false
EnableDebugMode : false
EnableHwWatchDogTimer : false
EnableRebootOnError : true
EnableTelnetServer : false
EnableRloginServer : false
EnableFtpServer : true
EnableTftpServer : false

VSP-9010:1#show software
=====
                        software releases in /intflash/release/
=====
3.3.3.0.GA (Backup Release)
3.4.0.0.GA (Primary Release)
-----
Auto Commit      : enabled
Commit Timeout   : 10 minutes
```

17. To confirm the secondary CP loaded and booted the correct version of software, look for the following messages on the master CP module:

```
CP2 [08/30/13 07:36:32.228] 0x00034594 00000000 GlobalRouter SW INFO
System boot
CP2 [08/30/13 07:36:32.228] 0x00034595 00000000 GlobalRouter SW INFO
VSP-9000 System Software Release 3.4.0.0
CP1 [08/30/13 07:36:37.488] 0x000105c8 00000000 GlobalRouter HW INFO HA-
CPU: Table Sync Completed on Secondary CPU
```

18. Use the **peer telnet** command to log in to the secondary CP and confirm the running software version:

```
VSP-9010:1#peer telnet
Trying 127.32.0.2 ...
Connected to 127.32.0.2
Escape character is '^]'

Copyright(c) 2010-2013 Avaya, Inc.
All Rights Reserved.
Virtual Services Platform 9000
Software Release Build 3.4.0.0
General Availability Released Software, Fully supported

AVAYA COMMAND LINE INTERFACE
```

```
Login: rwa
Password: ***
@VSP-9010:2>
```

Tips to replace a VSP 9012 with a VSP 9010

If you currently have a Virtual Services Platform 9012 in production and plan to replace it with a Virtual Services Platform 9010 due to the front to back cooling feature for your hot aisle/cold aisle data center, use the information in this section to identify and plan for key differences. You can reuse common hardware components such as power supplies, CP modules, and I/O modules.

The following table identifies key differences that you need to consider before you begin a replacement.

Requirement	Value	Notes
Software on the CP module	Release 3.3.3.0 or later	Releases prior to Release 3.3.3.0 do not detect the VSP 9010 chassis and will not boot. Releases 3.3.3.0 and later patches do detect the VSP 9010 chassis and boot to an upgrade menu. You must use a console connection to upgrade the software to Release 3.4 or later.
Chassis height	24.375 in. (61.91 cm) 14 rack units (RU)	The VSP 9010 is taller than the VSP 9012. Ensure you have adequate space in the rack. You can fit three VSP 9012 in a standard 19 inch wide, 7 foot tall rack. You can fit two VSP 9010 in a standard 19 inch wide, 7 foot tall rack.
I/O slot configuration	Supports slots 3 to 10.	The VSP 9010 does not provide a slot 11 or slot 12. You need to modify your configuration if you have I/O modules installed in slot 11 or 12 of a VSP 9012. If replacing an in-production VSP 9012 unit, you can modify the configuration offline, put it on the VSP 9010 using USB, FTP, or TFTP, and then boot it after you

Requirement	Value	Notes
		move modules into the new slots.
Cooling modules	1,900 W maximum for a pair of cooling modules	The cooling modules in the VSP 9010 require more power. Ensure you have enough available power remaining if you move power supplies from the VSP 9012. Use the show sys-info power command to determine the available power. If necessary, contact an Avaya sales representative for an offline power calculator.
9024XL module	Requires ventilation covers	If you install this module in a VSP 9010, you must use ventilation covers to prevent hot air discharge at the front of the chassis. For more information, see Using the VSP 9024XL Ventilation Cover for VSP 9010 on page 38.

9095SF module

The 9095SF Switch Fabric (SF) modules provide the back end switching solution in the midplane Virtual Services Platform 9010 chassis. Each 9095SF module connects to eight different interface modules and two CP modules simultaneously. Each chassis has slots for five operational SF modules plus one hot backup.

While the 9095SF modules are physically the same, the functions they perform vary based on the slots in which you install them. The SF slots 1 and 4 are for system operations and are called bandwidth managers.

The following table describes the functions of the SF modules based on their slot location.

Table 2: 9095SF module functions based on slot location

Slots	Function
SF1 and SF4	bandwidth manager
SF2, SF3, SF5, and SF6	X-bar switching function

*** Note:**

You must install a minimum of three SF modules in the chassis. Install an SF module in both slots SF1 and SF4. Install a third SF module in one of the remaining slots.

If you install a second bandwidth manager after a bandwidth manager failover, there is a small window where data can be lost. Perform this action during a maintenance window.

You can use the 9095SF module in the Virtual Services Platform 9010 chassis only.

9010CM cooling module

Install two cooling modules at the front of the Virtual Services Platform 9010 chassis, below the interface and CP modules. Each cooling module includes four fans. The Master CP module controls the fans depending on room temperature and the temperature of interface and SF modules installed in the chassis.

The air intake for the Virtual Services Platform 9010 chassis is below the cooling modules. The cooling modules cool all modules in the front of the chassis, as well as the Switch Fabric modules in the back.

You can use the 9010CM cooling module in the Virtual Services Platform 9010 chassis only.

Existing hardware supported in the current release

This section describes the hardware components of Avaya Virtual Services Platform 9000, and important notices or restrictions.

Virtual Services Platform 9012 chassis

The Virtual Services Platform 9012 chassis has 12 slots and 8 bays in the front and 8 slots and 2 bays in the back. Two front slots are for the CP module and ten front slots are for the interface modules. Six front bays are for the power supplies and two front bays are for interface cooling modules. Six back slots are for SF modules and two back slots are for future development. The two back bays are for SF cooling modules.

The following table provides the weight and dimensions of the Virtual Services Platform 9012 chassis.

Table 3: Virtual Services Platform 9012 chassis dimensions and weight

Width	17.5 in. (44.45 cm)
Height	24.375 in. (61.91 cm)

Depth	32.5 in. (82.55 cm) plus cable management system
Weight (chassis and midplane)	160 lb (73 kg)
Weight (chassis, midplane, and cooling modules)	183 lb (83 kg)

The Virtual Services Platform 9012 chassis also has the following features:

- Airflow is both side to side and front to back.
- Every module and power supply is hot swappable.
- The chassis has side handles on the bottom and top, and the front and back panels have handles to lift the Virtual Services Platform 9012 chassis.

9006AC power supply

The 9006AC power supply accepts 120 VAC nominal (90-140 VAC) or 220 VAC nominal (185–275 VAC) input.

With 120 VAC nominal input voltage conditions, the power supply produces a maximum of 1200 Watts of 54 VDC power. With 240 VAC nominal input voltage conditions, the power supply can output 2000 Watts of 54 VDC power.

You can use the 9006AC power supply in the Virtual Services Platform 9010AC and Virtual Services Platform 9012 chassis.

To determine how many power supplies you need, you can download *ERS 8000 / VSP 9000 Power Supply Calculator*, NN48500–519 from the **System Management & Planning** section of the Virtual Services Platform 9000 product documentation at <https://support.avaya.com>.

9012FC cooling module

The 9012FC cooling modules contain eight fans each to cool the interface modules. The 9012FC cooling module provides side-to-side cooling. You install them from the front of the Virtual Services Platform 9012 chassis.

You can use the 9012FC cooling module in the Virtual Services Platform 9012 chassis only.

9012RC cooling module

The 9012RC cooling modules contain two fans each to cool the SF modules. The 9012RC cooling module provides front-to-back cooling. You install them in the back of the Virtual Services Platform 9012 chassis.

You can use the 9012RC cooling module in the Virtual Services Platform 9012 chassis only.

The output for the `show sys-info card` command can incorrectly identify the module description as 9012SC. This description was programmed in the SEEPROM during manufacturing of early 9012RC cooling modules. These modules will continue to report this information. Newly manufactured modules correctly display 9012RC as the module description.

9024XL interface module

The 9024XL interface module is a 24 port 10 gigabit per second (Gb/s) small form-factor pluggable plus (SFP+) interface module.

The module has approximately a 3.5:1 oversubscribed line rate over 24 ports of 10 Gb/s Ethernet traffic using standard SFP+ fiber transceivers. Each continuous physical group of 4 ports supports a combined bandwidth of 11.3GE. Use only a single port for each grouping to ensure no oversubscription. As a helpful guide the last port in each group has a black mark on the faceplate.

The module supports a maximum throughput of 105 Mpps over 24 ports of 10 Gb/s Ethernet traffic using standard SFP+ fiber transceivers. The module supports SR, LR, LRM, ER, and ZR SFP+ transceivers.

The following table provides the multimode fiber (MMF), single-mode fiber (SMF), and copper SFP and SFP+ fiber transceivers that the 9024XL module supports.

! Important:

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

Table 4: Supported SFP and SFP+ fiber transceivers for the 9024XL module

Model number	Part number	Description
10GBASE-SR/SW	AA1403015-E6	850 nanometers (nm). The range is up to the following: <ul style="list-style-type: none"> • 26 m using 62.5 micrometer (µm), 160 megaHertz times km (MHz-km) MMF • 33 m using 62.5 µm, 200 MHz-km MMF • 66 m using 62.5 µm, 400 MHz-km MMF • 82 m using 50 µm, 500 MHz-km MMF

Model number	Part number	Description
		<ul style="list-style-type: none"> • 300 m using 50 μm, 2000 MHz-km MMF • 400 m using 50 μm, 4700 MHz-km MMF (OM4)
10GBASE-LRM	AA1403017-E6	1310 nm. Up to 220 m reach over Fiber Distributed Data Interface (FDDI)-grade 62.5 μ m multimode fiber. Suited for campus LANs.
10GBASE-LR/LW	AA1403011-E6	1310 nm SMF. The range is up to 10 km.
10GBASE-ER/EW	AA1403013-E6	1550 nm SMF. The range is up to 40 km.
10GBASE-ER CWDM DDI	AA1403153-E6	1471 nm SMF. The range is up to 40 km.
	AA1403154-E6	1491 nm SMF. The range is up to 40 km.
	AA1403155-E6	1511 nm SMF. The range is up to 40 km.
	AA1403156-E6	1531 nm SMF. The range is up to 40 km.
	AA1403157-E6	1551 nm SMF. The range is up to 40 km.
	AA1403158-E6	1571 nm SMF. The range is up to 40 km.
	AA1403159-E6	1591 nm SMF. The range is up to 40 km.
	AA1403160-E6	1611 nm SMF. The range is up to 40 km.
10GBASE-ZR/ZW	AA1403016-E6	1550 nm SMF. The range is up to 70 km.
10GBASE-ZR CWDM DDI	AA1403161-E6	1471 nm SMF. The range is up to 70 km.
	AA1403162-E6	1491 nm SMF. The range is up to 70 km.
	AA1403163-E6	1511 nm SMF. The range is up to 70 km.
	AA1403164-E6	1531 nm SMF. The range is up to 70 km.

Model number	Part number	Description
	AA1403165-E6	1551 nm SMF. The range is up to 70 km.
	AA1403166-E6	1571 nm SMF. The range is up to 70 km.
	AA1403167-E6	1591 nm SMF. The range is up to 70 km.
	AA1403168-E6	1611 nm SMF. The range is up to 70 km.
10GBASE-CX	AA1403018-E6 to AA1403021-E6	4-pair twinaxial copper cable to connect 10 Gb ports. The maximum range is 15 m.
1000BASE-SX DDI	AA1419048-E6	Well-suited for campus local area networks (LAN) and intrabuilding links. Up to 275 or 550 m reach (fiber-dependent) over a fiber pair.
1000BASE-LX DDI	AA1419049-E6	The range is up to to 10 km reach over a single mode fiber (SMF) pair. The range is up to 550 m reach over a multimode fiber (MMF) pair.
1000BASE-XD DDI	AA1419050-E6	1310 nm. The range is up to 40 km over SMF pair.
	AA1419051-E6	1550 nm (non-CWDM). The range is up to 40 km over SMF pair.
1000BASE-ZX DDI	AA1419052-E6	1550 nm (non-CWDM). The range is up to 70 km over SMF pair.
1000BASE-BX-U	AA1419069-E6	1310 nm, up to 10km
	AA1419076-E6	1310 nm, up to 40km
1000BASE-BX-D	AA1419070-E6	1490 nm, up to 10km
	AA1419077-E6	1490 nm, up to 40km
1000BASE-EX DDI	AA1419071-E6	1550 nm, up to 120 km (non-CWDM)
1000BASE DDI CWDM	AA1419053-E6	1470 nm (CWDM). The range is up to 40km over SMF pair.
1000BASE DDI CWDM	AA1419054-E6	1490 (CWDM). The range is up to 40km over SMF pair.

Model number	Part number	Description
1000BASE DDI CWDM	AA1419055-E6	1510 nm (CWDM). The range is up to 40km over SMF pair.
1000BASE DDI CWDM	AA1419056-E6	1530 nm (CWDM). The range is up to 40km over SMF pair.
1000BASE DDI CWDM	AA1419057-E6	1550 nm (CWDM). The range is up to 40km over SMF pair.
1000BASE DDI CWDM	AA1419058-E6	1570 nm (CWDM). The range is up to 40km over SMF pair.
1000BASE DDI CWDM	AA1419059-E6	1590 nm (CWDM). The range is up to 40km over SMF pair.
1000BASE DDI CWDM	AA1419060-E6	1610 nm (CWDM). The range is up to 40km over SMF pair.
1000BASE DDI CWDM	AA1419061-E6	1470 nm (CWDM). The range is up to 70km over SMF pair.
1000BASE DDI CWDM	AA1419062-E6	1490 nm (CWDM). The range is up to 70km over SMF pair.
1000BASE DDI CWDM	AA1419063-E6	1510 nm (CWDM). The range is up to 70km over SMF pair.
1000BASE DDI CWDM	AA1419064-E6	1530 nm (CWDM). The range is up to 70km over SMF pair.
1000BASE DDI CWDM	AA1419065-E6	1550 nm (CWDM). The range is up to 70km over SMF pair.
1000BASE DDI CWDM	AA1419066-E6	1570 nm (CWDM). The range is up to 70km over SMF pair.
1000BASE DDI CWDM	AA1419067-E6	1590 nm (CWDM). The range is up to 70km over SMF pair.
1000BASE DDI CWDM	AA1419068-E6	1610 nm (CWDM). The range is up to 70km over SMF pair.

Model number	Part number	Description
1000BASE-T	AA1419043-E6	CAT5 UTP, up to 100 m. Because the 1000BASE-T device is all electrical, it does not need DDI support.

The 9024XL interface module has a 1 GHz 8584E processor and 1 GB onboard DDR2 memory.

You can use the 9024XL module in both the Virtual Services Platform 9010 and Virtual Services Platform 9012 chassis.

The 9024XL 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

Using the VSP 9024XL Ventilation Cover for VSP 9010

Use the following information to ensure proper airflow in your chassis. The 9024XL module has six sets of SFP+ cages through the front panel with ventilation above or below each set of SFP+ cages.

About this task

Virtual Services Platform 9012:

When you install the 9024XL module in the Virtual Services Platform 9012 chassis, you must remove the ventilation cover.

The Virtual Services Platform 9012 draws cool air from front to back and from left to right. When the 9024XL module is in the Virtual Services Platform 9012, the open front perforations allow for additional air movement.

Virtual Services Platform 9010:

When you install the 9024XL module in the Virtual Services Platform 9010 it is best to cover the front perforations for improved airflow.

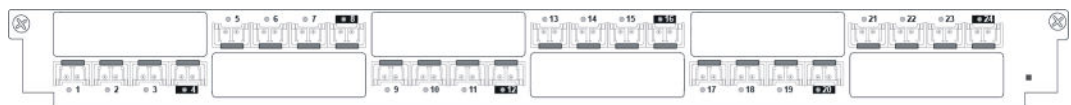
When you install a 9024XL module in the Virtual Services Platform 9010, attach the VSP 9024XL Ventilation Cover for VSP 9010 to the open sections at the front of the module. The ventilation cover attaches over the front of the module to direct hot air from the module into the hot aisle, and ensure the modules and chassis remain cool. The Virtual Services Platform 9010 draws cool air from front to back.

If you do not attach the ventilation cover to the front of the 9024XL module in the Virtual Services Platform 9010, hot air from the modules can be exhausted into the cool aisle in the room.

The Virtual Services Platform 9010 ships with eight covers, which is enough for eight modules. If you need replacement ventilation covers, you can order a new cover using order code EC1411016-E6.

Procedure

1. Remove the paper backing from the sticker.
2. Align the adhesive side of the sticker with the module faceplate so that the vents are covered and the ports are exposed.
3. Firmly press the sticker over each vent location to ensure full adherence.
4. Grasp the tab on one end of the sticker and slowly pull in the opposite direction to leave only the six ventilation covers in place.



9048GB interface module

The 9048GB interface module is a 48 port 1 Gb/s small form-factor pluggable (SFP) interface module that supports multimode fiber (MMF), single-mode fiber (SMF), and copper connections.

The following table details the SFP transceivers supported by the 9048GB module.

! Important:

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

Table 5: Supported SFP transceivers for the 9048GB module

Model	ROHS product number	Description
1000BASE-T	AA1419043-E6	CAT5 UTP, up to 100 m. Because the 1000BASE-T device is all electrical, it does not need DDI support.
1000BASE-SX DDI	AA1419048-E6	850 nm up to 275 m using 62.5 m MMF optic cable up to 550 m using 50 μ m MMF optic cable

Model	ROHS product number	Description
1000BASE-LX DDI	AA1419049-E6	1310 nm, up to 10 km
1000BASE-XD DDI	AA1419050-E6	1310 nm, up to 40 km
	AA1419051-E6	1550 nm, up to 40km (non-CWDM)
1000BASE-ZX DDI	AA1419052-E6	1550 nm, up to 70 km (non-CWDM)
1000BASE-BX-U	AA1419069-E6	1310 nm, up to 10km
	AA1419076-E6	1310 nm, up to 40km
1000BASE-BX-D	AA1419070-E6	1490 nm, up to 10km
	AA1419077-E6	1490 nm, up to 40km
1000BASE-EX DDI	AA1419071-E6	1550 nm, up to 120 km (non-CWDM)
1000BASE DDI CWDM	AA1419053-E6	1470 nm, up to 40 km
	AA1419054-E6	1490 nm, up to 40 km
	AA1419055-E6	1510 nm, up to 40 km
	AA1419056-E6	1530 nm, up to 40 km
	AA1419057-E6	1550 nm, up to 40 km
	AA1419058-E6	1570 nm, up to 40 km
	AA1419059-E6	1590 nm, up to 40 km
	AA1419060-E6	1610 nm, up to 40 km
	AA1419061-E6	1470 nm, up to 70 km
	AA1419062-E6	1490 nm, up to 70 km
	AA1419063-E6	1510 nm, up to 70 km
	AA1419064-E6	1530 nm, up to 70 km
	AA1419065-E6	1550 nm, up to 70 km
	AA1419066-E6	1570 nm, up to 70 km
	AA1419067-E6	1590 nm, up to 70 km
AA1419068-E6	1610 nm, up to 70 km	
100BASE-FX	AA1419074-E6	1310 nm, up to 2km

The 9048GB is 100/1000 Mb/s capable.

The 9048GB has a 1 GHz 8584E processor and 1 GB onboard DDR2 memory. This module has a maximum throughput of 70 Mpps.

The 9048GB has the following characteristics:

- compliant with IEEE 802.3z standards
- 802.3 Ethernet frame format, MAC layer functionality
- asynchronous Ethernet interface

You can use the 9048GB module in the Virtual Services Platform 9010 and Virtual Services Platform 9012.

9048GT interface module

The 9048GT interface module is a 48 port 10/100/1000M Ethernet Copper interface module with RJ45 connectors.

The 9048GT interface module has a 1 GHz 8584E processor and 1 GB onboard DDR2 memory. This module has a maximum throughput of 70 Mpps.

The 9048GT has the following characteristics:

- compliant with IEEE 802.3ab standards
- 802.3 Ethernet frame format, MAC layer functionality
- asynchronous Ethernet interface

You can use the 9048GT module in the Virtual Services Platform 9010 and Virtual Services Platform 9012 chassis.

9080CP Control Processor module

The 9080CP CP module runs all high level protocols, and distributes the results (routing updates) to the rest of the system, manages and configures the interface and SF modules, and maintains and monitors the health of the chassis.

The 9080CP module contains two 8542E Control Processor Units (CPU) running at 1.33 gigahertz (GHz). Each processor comes with two double-data-rate two (DDR2) dual in-line memory module (DIMM) of memory, for a maximum of 4 GB Random Access Memory (RAM) for each processor. The 9080CP module measures 23 inches in length.

The 9080CP module supports the following interfaces:

- console port, DB9
- ethernet management, RJ45
- Universal Serial Bus (USB) type A (Master)
- external Compact Flash

The external Compact Flash card is mandatory. The following table lists the external storage devices you can order to use with the CP module.

Table 6: Supported external storage devices

Model number	Description
EC1411011-E6	2GB USB memory flash drive
EC1411010-E6	2GB Compact Flash memory card

*** Note:**

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

You can hot swap the external storage devices but you must follow a specific procedure to avoid data loss or hardware damage. To properly remove an external storage device, see [Removing external storage devices from the CP module](#) on page 44.

The 9080CP module has light-emitting-diodes (LED) duplicating the LEDs of the modules in the back of the chassis.

The LEDs map differently depending on the chassis in which you install the CP module. Software on the 9080CP module automatically determines whether you install the 9080CP module into the Virtual Services Platform 9010 chassis or the Virtual Services Platform 9012 chassis. You do not have to update the configuration. For more information on LED mapping for each chassis, see *Avaya Virtual Services Platform 9000 Installation — Modules*, NN46250–301.

You can see the following intermittent error on the CP module after a reboot or an HA failover:

```
ERROR: [bcmScoreboard.0]SB_FLIB(V0): [bcmScoreboard.0]QM_ERROR2,
FB_TAIL_CACHE_OVERFLOW Set
```

You can ignore this message. The message has no functional impact on the system.

Redundancy:

The 9080CP module architecture provides redundancy if you use two CP modules in a system.

⚠ Caution:

Risk of file system corruption

To remove a master CP module from the chassis, you must follow the Avaya recommended procedure, [Removing a master CP module with CPU-HA mode activated](#) on page 44. Failure to follow this procedure can result in file system corruption.

You can use the 9080CP module in the Virtual Services Platform 9010 and Virtual Services Platform 9012 chassis.

! **Important:**

The CP modules in the Virtual Services Platform 9010AC chassis must use a minimum software version of Release 3.4.

9090SF Switch Fabric module

The 9090SF Switch Fabric (SF) modules provide the back end switching solution in the midplane Virtual Services Platform 9012 chassis. Each 9090SF module connects to ten different interface modules and two CP modules simultaneously. Each chassis has slots for five operational SF modules plus one hot backup. The 9090SF modules measure 15.5 inches in length.

While the 9090SF modules are physically the same, the functions they perform vary based on the slots in which you install them. The SF slots 1 and 4 are for system operations and are called bandwidth managers.

The following table details the functions of the SF modules based on their slot location.

Table 7: 9090SF module functions based on slot location

Slots	Function
SF1 and SF4	bandwidth manager
SF2, SF3, SF5, and SF6	X-bar switching function

*** Note:**

You must install a minimum of three SF modules in the chassis. Install an SF module in both slots SF1 and SF4. Install a third SF module in one of the remaining slots.

If you install a second bandwidth manager after a bandwidth manager failover, there is a small window where data can be lost. Perform this action during a maintenance window.

The 9024XL has a throughput capability of 105 Mpps when the chassis is equipped with 5 SF modules. The 9048GB and 9048GT modules have a throughput capability of 70 Mpps when the chassis is equipped with 5 SF modules.

You can use the 9090SF module in the Virtual Services Platform 9012 chassis only.

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 USB and 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 USB or 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 VSP 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

```
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

File names for this release

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 8: Software files

File name	Description	Size (bytes)
VSP9K.3.4.0.2.tgz	Release 3.4 archived distribution	114,686,742
VSP9K.3.4.0.2_modules.tgz	Encryption modules	41,899

! 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 9: Open Source software files

File name	Description	Size (bytes)
VSP9K.3.4.0.1_oss-notice.html	Master copyright file. This file is located in the Licenses directory.	414,245
VSP9K.3.4.0.2_OpenSource.zip	Open source base software for Virtual Services Platform 9000 Release 3.4.	96,168,559

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

 **Caution:**

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

 **Caution:**

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.

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 8.x and 9.x

Environmental specifications

The following table provides the minimum and maximum environmental specifications for Virtual Services Platform 9000 operation.

Table 10: Minimum and maximum operational environmental specifications

Operating environmental specification	VSP 9010 chassis		VSP 9012 chassis	
	Minimum	Maximum	Minimum	Maximum
Temperature	0°C	40°C (see note below)	0°C	40°C (see note below)
<p> Note: With 9024XL modules with serial numbers starting with LBNNTMC9xxxxxx, the operating temperature is 0-38°C.</p>				
Relative humidity	—	85%	10%	90%
Altitude	—	10,000 ft	0 ft	10,000 ft
Thermal shock	-40°C	85°C	-40°C	85°C
Vibration, peak to peak displacement	—	0.005 in. (5 to 32 Hz)	—	0.005 in. (5 to 32 Hz)
Audible noise	83 dB	105 dB	75 dB	89 dB

The following table provides the minimum and maximum environmental specifications for storage of the Virtual Services Platform 9000.

Table 11: Minimum and maximum storage environmental specifications

Storage environmental parameter	VSP 9010 chassis		VSP 9012 chassis	
	Minimum	Maximum	Minimum	Maximum
Temperature	-10°C	60°C	-10°C	60°C
Relative humidity	—	90%	—	90%
Altitude	—	10,000 ft	—	10,000 ft

The following table lists the operational requirements of an unpackaged Virtual Services Platform 9000.

Table 12: Unpackaged operational requirements for the VSP 9010 and VSP 9012 chassis

Unpackaged operational requirements	Standard specification	Note
Operational vibration (Sinusoidal)	European Telecommunications Standard (ETS) 300 019-1-3 and International	Shock of low significance, such as slamming door

Unpackaged operational requirements	Standard specification	Note
	Electrotechnical Commission (IEC) 68-2-6 test Fc	
Shock 30g 11ms	International Electrotechnical Commission (IEC) 68-2-27	Shock of low significance

The following tables list the requirements of a packaged Virtual Services Platform 9000 for storage and transport.

Table 13: Packaged nonoperational requirements for the VSP 9012 chassis.

Packaged nonoperational requirements (storage and transport)	Standard specification	Note
Transportation vibration (Sinusoidal)	Bellcore GR-63-Core issue 1 Oct 1995	All kinds of trucks and trailers, trains, ships; well-developed roads
Transportation bounce (4 inch drop onto normal rest face, 2 edges and 2 corners)	IEC 68-2-31 or Bellcore GR-63-CORE, issue 1 Oct 1995	Transportation handling
Package drop (Package weight less than 20 kg. Drop onto 3 faces, 3 edges and 3 corners from a height of 75 cm.)	Bellcore GR-63-CORE issue 1 Oct 1995	Transportation handling

Table 14: Packaged nonoperational requirements for the VSP 9010 chassis.

Packaged nonoperational requirements (storage and transport)	Standard specification	Note
Transportation vibration (Individually palletized product. Package weight more than 150 lbs [68 kg])	ASTM D4169 assurance level 2	All kinds of mechanical equipment; well-developed roads
Package impact	ASTM D5277	Transportation handling

Reliability

The following table lists the mean time between failures of the various modules of the Virtual Services Platform 9000.

Table 15: Reliability

Component	Mean time between failures
VSP 9010 AC chassis	500,000 hours
VSP 9012 chassis	500,000 hours
Fan tray module for VSP 9010 chassis	500,000 hours
Fan tray modules for VSP 9012 chassis	500,000 hours
9006AC power supply	400,000 hours
9090SF module	1,450,000 hours
9095SF module	1,450,000 hours
9080CP module	777,000 hours
Interface modules	<ul style="list-style-type: none"> • 9024XL — 210,000 hours • 9048GB — 268,000 hours • 9048GT — 279,000 hours

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 *Avaya Virtual Services Platform 9000 Administration*, NN46250–600.

Supported system and management applications with IPv6

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 *Avaya Virtual Services Platform 9000 Administration*, 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 *Avaya Virtual Services Platform 9000 Upgrades and Patches*, 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 *Avaya Virtual Services Platform 9000 Administration*, NN46250–600.

Fixes from previous releases

The Virtual Services Platform 9000 Software Release 3.4 incorporates all fixes from prior releases, up to and including, Release 3.3.4.1.

Hardware and software compatibility

This section describes the hardware and the minimum software version required to support the hardware. The following table provides information for Virtual Services Platform 9010. For information on Virtual Services Platform 9012, see [Hardware and minimum software version for the VSP 9012](#) on page 57.

Table 16: Hardware and minimum software version for the VSP 9010


Chassis, switching fabrics, and control processors		Minimum software version	Part number
VSP 9010 AC	10-slot chassis (AC input)	3.4	EC1402002-E6
9080CP	Control Processor module	The 9080CP must run the software version required for installed components. See the minimum version required for the components you install.	EC1404007-E6
Note that Release 3.3.3.0 is the required baseline to upgrade a CP module in a VSP 9010 chassis to Release 3.4.0.0.			

Chassis, switching fabrics, and control processors		Minimum software version	Part number
9095SF	Switch Fabric module for the VSP 9010	3.4	EC1404009-E6
Power supplies			
9006AC	1,200-2,000 W AC power supply	3.4	EC1405A01-E6
Cooling modules			
9010CM	Front-to-back cooling for the VSP 9010	3.4	EC1411012-E6
Ethernet modules			
9024XL	24-port 10GBASE-X SFP +/SFP	3.4	EC1404001-E6
9048GB	48-port 1000BASE-X SFP	3.4	EC1404002-E6
9048GT	48-port 10/100/1000BASE-T	3.4	EC1404003-E6
Compatible SFPs and SFP+s For more information about SFPs and SFP+s, see <i>Avaya Virtual Services Platform 9000 Installation — SFP Hardware Components</i> , NN46250-305			
100BASE-FX SFP	1310 nm, 100 Mb/s Ethernet, multimode fiber, duplex LC connector	3.4	AA1419074-E6
1000BASE-T SFP	Gigabit Ethernet, RJ-45 connector	3.4	AA1419043-E6
1000BASE-SX DDI SFP	850 nm, Gigabit Ethernet, duplex LC connector	3.4	AA1419048-E6
1000BASE-LX DDI SFP	1310 nm, Gigabit Ethernet, duplex LC connector	3.4	AA1419049-E6
1000BASE-XD DDI SFP	1310 nm, Gigabit Ethernet, duplex LC connector	3.4	AA1419050-E6
	1550 nm, Gigabit Ethernet, duplex LC connector		AA1419051-E6
1000BASE-ZX DDI SFP	1550 nm, Gigabit Ethernet, duplex LC connector	3.4	AA1419052-E6
1000BASE-BX DDI SFP	1310 nm (tx) and 1490 nm (rx), 1490 nm (tx) 1310 nm (rx), Gigabit Ethernet, single-fiber LC connector,	3.4	AA1419069-E6 (10 km at 1310 nm) AA1419076-E6 (40 km at 1310 nm)

Chassis, switching fabrics, and control processors		Minimum software version	Part number
			AA1419070-E6 (10 km at 1490 nm) AA1419077-E6 (40 km at 1490 nm)
1000BASE-EX DDI SFP	1550 nm, Gigabit Ethernet, duplex LC connector	3.4	AA1419071-E6
1000BASE DDI CWDM 40 km SFP	Gigabit Ethernet, duplex LC connector	3.4	AA1419053-E6 to AA1419060-E6
1000BASE DDI CWDM 70 km SFP	Gigabit Ethernet, duplex LC connector	3.4	AA1419061-E6 to AA1419068-E6
10GBASE-SR/SW SFP+	400 m, 850nm MMF	3.4	AA1403015-E6
10GBASE-LRM SFP+	220 m, 1260 to 1355 nm; 1310 nm nominal MMF,	3.4	AA1403017-E6
10GBASE-LR/LW SFP+	10 km, 1310nm SMF	3.4	AA1403011-E6
10GBASE-ER/EW SFP+	40 km, 1550nm SMF	3.4	AA1403013-E6
10GBASE-ER CWDM DDI SFP+	40 km, 1471 to 1611 nm.	3.4	AA1403153-E6 to AA1403160-E6
10GBASE-CX	4-pair twinaxial copper cable that plugs into the SFP+ socket and connects two 10 Gb ports.	3.4	AA1403018-E6 to AA1403021-E6
10GBASE-ZR/ZW	80 km, 1550nm SMF	3.4	AA1403016-E6
10GBASE-ZR CWDM DDI SFP+	70 km, 1471 to 1611 nm	3.4	AA1403161-E6 to AA1403168-E6

The following table provides information for Virtual Services Platform 9012.

Table 17: Hardware and minimum software version for the VSP 9012

Chassis, switching fabrics, and control processors		Minimum software version	Part number
VSP 9012	12-slot chassis	3.0	EC1402001-E6
9080CP	Control Processor module	The 9080CP must run the software version required for installed components. See the minimum version required for the components you install.	EC1404007-E6
9090SF	Switch Fabric module for the VSP 9012	3.0	EC1404006-E6
Power supplies			
9006AC	1,200-2,000 W AC power supply	3.0.	EC1405A01-E6
Cooling modules			
9012FC	Side-to-side cooling for the VSP 9012	3.0	EC1411001-E6
9012RC	Front-to-back cooling for the VSP 9012	3.0	EC1411002-E6
Ethernet modules			
9024XL	24-port 10GBASE-X SFP +/SFP	See the following note.	EC1404001-E6
9048GB	48-port 1000BASE-X SFP		EC1404002-E6
9048GT	48-port 10/100/1000BASE-T		EC1404003-E6
<p> Note:</p> <p>The CP module must run a minimum of one of the following software versions to support the 9024XL, 9048GB, or 9048GT interface modules in a VSP 9012:</p> <ul style="list-style-type: none"> • 3.1.1.0 with patch VSP9K.3.1.1.0.GA-T01028195A.tgz • 3.2.0.0 with patch VSP9K.3.2.0.0.GA-T01020549A.tgz • 3.3.0.0 with patch VSP9K.3.3.0.0.GA-T01028199A.tgz 			

Chassis, switching fabrics, and control processors		Minimum software version	Part number
<ul style="list-style-type: none"> • 3.3.1.0 with patch VSP9K.3.3.1.0.GA-T01029789A.tgz • 3.3.2.0 and later 			
<p>Compatible SFPs and SFP+s For more information about SFPs and SFP+s, see <i>Avaya Virtual Services Platform 9000 Installation — SFP Hardware Components</i>, NN46250-305.</p>			
100BASE-FX SFP	1310 nm, 100 Mb/s Ethernet, multimode fiber, duplex LC connector	3.0	AA1419074-E6
1000BASE-T SFP	Gigabit Ethernet, RJ-45 connector	3.0	AA1419043-E6
1000BASE-SX DDI SFP	850 nm, Gigabit Ethernet, duplex LC connector	3.0	AA1419048-E6
1000BASE-LX DDI SFP	1310 nm, Gigabit Ethernet, duplex LC connector	3.0	AA1419049-E6
1000BASE-XD DDI SFP	1310 nm, Gigabit Ethernet, duplex LC connector	3.0	AA1419050-E6
	1550 nm, Gigabit Ethernet, duplex LC connector	3.0	AA1419051-E6
1000BASE-ZX DDI SFP	1550 nm, Gigabit Ethernet, duplex LC connector	3.0	AA1419052-E6
1000BASE-BX DDI SFP	1310 nm (tx) and 1490 nm (rx), 1490 nm (tx) 1310 nm (rx), Gigabit Ethernet, single-fiber LC connector	3.0	AA1419069-E6 (10 km at 1310 nm) AA1419076-E6 (40 km at 1310 nm) AA1419070-E6 (10 km at 1490 nm) AA1419077-E6 (40 km at 1490 nm)
1000BASE-EX DDI SFP	1550 nm, Gigabit Ethernet, duplex LC connector	3.0	AA1419071-E6
1000BASE DDI CWDM 40 km SFP	Gigabit Ethernet, duplex LC connector	3.0	AA1419053-E6 to AA1419060-E6
1000BASE DDI CWDM 70 km SFP	Gigabit Ethernet, duplex LC connector	3.0	AA1419061-E6 to

Chassis, switching fabrics, and control processors		Minimum software version	Part number
			AA1419068-E6
10GBASE-SR/SW SFP+	400m, 850nm MMF	3.0	AA1403015-E6
10GBASE-LRM SFP+	220 m, 1260 to 1355 nm; 1310 nm nominal MMF	3.0	AA1403017-E6
10GBASE-LR/LW SFP+	10km, 1310nm SMF	3.0	AA1403011-E6
10GBASE-ER/EW SFP+	40km, 1550nm SMF	3.0	AA1403013-E6
10GBASE-ER CWDM DDI SFP+	40 km, 1471 to 1611 nm	3.4	AA1403153-E6 to AA1403160-E6
10GBASE-CX	4-pair twinaxial copper cable that plugs into the SFP+ socket and connects two 10 Gb ports	3.0	AA1403018-E6 to AA1403021-E6
10GBASE-ZR/ZW	70km, 1550nm SMF	3.4	AA1403016-E6
10GBASE-ZR CWDM DDI SFP+	70 km, 1471 to 1611 nm	3.4	AA1403161-E6 to AA1403168-E6

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
<i>Switch Clustering using Split-MultiLink Trunking (SMLT) with VSP 9000, ERS 8600/8800, 8300, and 5000 Technical Configuration Guide</i>	NN48500-518

Document title	Document number
<i>Switch Clustering Supported Topologies and Interoperability with Virtual Services Platform 9000 & Ethernet Routing Switches</i>	NN48500-555
<i>Technical Configuration Guide for Microsoft Network Load Balancing</i>	NN48500-593
<i>Super Large Campus Technical Configuration Guide</i>	NN48500-609
<i>Avaya Virtual Services Platform 9000 with Coraid EtherDrive SRX-Series Storage Appliances Technical Configuration Guide</i>	NN48500-611
<i>Avaya Flare™ for Avaya Data Technical Configuration Guide</i>	NN48500-613
<i>Shortest Path Bridging (802.1aq) for ERS 8800 and VSP 9000 Technical Configuration Guide</i>	NN48500-617
<i>Migrating to a Virtual Services Fabric using Shortest Path Bridging Technical Configuration Guide</i>	NN48500-622
<i>Avaya Virtual Services Platform 9000 and Avaya Virtual Services Platform 7000 with Coraid EtherDrive SRX-Series Storage Appliances Technical Configuration Guide</i>	NN48500-629
<i>Basic SPB Configuration</i>	NN48500-632
<i>IPv6 for VSP 9000 Technical Configuration Guide</i>	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 *Avaya Virtual Services Platform 9000 Release Notes*, 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 18: Module capabilities

Component	Maximum number supported
9024XL I/O module	
10GbE fiber connections	9010 chassis: 192 (8 x 24) 9012 chassis: 240 (10 x 24)
Processor	1 GHz
9048GB I/O module	
GbE fiber connections	9010 chassis: 384 (8 x 48) 9012 chassis: 480 (10 x 48)
Processor	1 GHz
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

Component	Maximum number supported
External Compact Flash	1 per CP module

Table 19: VSP 9010 AC chassis capabilities

Component	Maximum number supported
CP modules	2
Interface modules	8
SF modules	6 You must install a minimum of 3 SF modules in the chassis.
Power Supplies	8
Total power capacity	<ul style="list-style-type: none"> • 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 20: VSP 9012 chassis capabilities

Component	Maximum number supported
CP modules	2
Interface modules	10
SF modules	6 You must install a minimum of 3 SF modules in the chassis.
Auxiliary slots	2
Power supplies	6
Total power capacity	<ul style="list-style-type: none"> • 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 21: Software scaling capabilities

	Maximum number supported
<i>Layer 2</i>	
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
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
Source MAC-based VLANs	100
Split Multi-Link Trunking (SMLT)	511 groups plus 1 IST MLT
SMLT ports per group	16
VLACP Interfaces	128
<i>Layer 3</i>	
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
Circuitless IP interfaces	256
ECMP routes	64,000
ECMP routes (fastpath)	8
FIB IPv4 routes	500,000
FIB IPv6 routes	128,000

	Maximum number supported
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. The maximum number of 500,000 IPv4 routes is possible when no IPv6 routes are configured, and the maximum number of IPv6 routes is 128,000 when no IPv4 routes are configured.	
IPv4 interfaces	4,343
IP interfaces (Router)	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
IPv4 or IPv6 Rlogin sessions	8 each, 16 total
IPv4 or IPv6 SSH sessions	8 total (any combination of IPv4 and IPv6 up to 8)
IPv4 or IPv6 Telnet sessions	8 each, 16 total
IPv4 VRF instances	512
IPv6 dynamic neighbors/interface	64K
IPv6 interfaces	4,087 (4,084 VLAN and 3 management [1/1, 2/1, virtual IP])
IPv6 routes (fastpath)	128,000
IPv6 static neighbors	1,000
IPv6 static routes	10,000
IPv6 tunnels	2,000
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

	Maximum number supported
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
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
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
VRRP interfaces fast timers (200ms)	24
<i>Diagnostics</i>	
Mirrored ports	479
Remote Mirroring Termination (RMT) ports	32

	Maximum number supported
<i>Filters and QoS</i>	
Flow-based policers (IPv4 and IPv6)	16,000
Port shapers (IPv4 and IPv6)	480
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
<i>SPBM</i>	
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	64
Layer 2 VSNs	4,000
VLANs in VRF	1,600
Layer 3 VSNs	512

Chapter 5: Supported standards, request for comments, and Management Information Bases

This chapter details the standards, request for comments (RFC), and Management Information Bases (MIB) that Avaya Virtual Services Platform 9000 supports.

Supported standards

The following table details the standards that Avaya Virtual Services Platform 9000 supports.

Table 22: Supported standards

Standard	Description
802.1ag	Connectivity Fault Management
802.1ah	Provider Backbone Bridges (MacInMac encapsulation)
802.1aq	Shortest Path Bridging (SPB)
802.1AX	Link Aggregation Control Protocol (LACP)
802.1D	MAC bridges (Spanning Tree)
802.1p	VLAN prioritization
802.1Q	Virtual Local Area Network (VLAN) tagging
802.1Qbb	Virtual Bridged Local Area Networks - Amendment: Priority-based Flow Control
802.1s	Multiple Spanning Tree Protocol (MSTP)
802.1t	802.1D maintenance
802.1v	VLAN Classification by Protocol and Port
802.1w-2001	Rapid Spanning Tree protocol (RSTP)
802.1X	Extensible Authentication Protocol (EAP), and EAP over LAN (EAPoL)
802.1X-2004	Port Based Network Access Control

Standard	Description
802.3 CSMA/CD Ethernet ISO/IEC 8802	International Organization for Standardization (ISO) /International Eletrotechnical Commission (IEC) 8802-3
802.3ab	Gigabit Ethernet 1000BaseT 4 pair Category 5 (Cat5) Unshieled Twisted Pair (UTP)
802.3ae	10 Gigabit Ethernet
802.3an	10 Gigabit Copper
802.3i	10BaseT
802.3u	100BaseT
802.3x	flow control
802.3z	Gigabit Ethernet

Supported RFCs

The following table and sections list the RFCs that Avaya Virtual Services Platform 9000 supports.

Table 23: Supported request for comments

Request for comment	Description
draft-grant-tacacs-02.txt	TACACS+ Protocol
RFC 768	UDP Protocol
RFC 783	Trivial File Transfer Protocol (TFTP)
RFC 791	Internet Protocol (IP)
RFC 792	Internet Control Message Protocol (ICMP)
RFC 793	Transmission Control Protocol (TCP)
RFC 826	Address Resolution Protocol (ARP)
RFC 854	Telnet protocol
RFC 894	A standard for the Transmission of IP Datagrams over Ethernet Networks
RFC 896	Congestion control in IP/TCP internetworks
RFC 903	Reverse ARP Protocol
RFC 906	Bootstrap loading using TFTP
RFC 950	Internet Standard Subnetting Procedure

Request for comment	Description
RFC 951	BootP
RFC 959, RFC 1350, and RFC 2428	IPv6 FTP and TFTP client and server
RFC 1027	Using ARP to implement transparent subnet gateways/Nortel Subnet based VLAN
RFC 1058	RIPv1 Protocol
RFC 1112	IGMPv1
RFC 1122	Requirements for Internet Hosts
RFC 1253	OSPF
RFC 1256	ICMP Router Discovery
RFC 1258	IPv6 Rlogin server
RFC 1305	Network Time Protocol v3 Specification, Implementation and Analysis
RFC 1340	Assigned Numbers
RFC 1519	Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC1541	Dynamic Host Configuration Protocol1
RFC1542	Clarifications and Extensions for the Bootstrap Protocol
RFC 1583	OSPFv2
RFC 1587	The OSPF NSSA Option
RFC 1591	DNS Client
RFC 1723	RIP v2 – Carrying Additional Information
RFC 1745	BGP / OSPF Interaction
RFC 1771 and RFC 1772	BGP-4
RFC 1812	Router requirements
RFC 1866	HyperText Markup Language version 2 (HTMLv2) protocol
RFC 1965	BGP-4 Confederations
RFC 1966	BGP-4 Route Reflectors
RFC 1981	Path MTU discovery
RFC 1997	BGP-4 Community Attributes
RFC 1998	An Application of the BGP Community Attribute in Multi-home Routing

Request for comment	Description
RFC 2068	Hypertext Transfer Protocol
RFC 2131	Dynamic Host Control Protocol (DHCP)
RFC 2138	RADIUS Authentication
RFC 2139	RADIUS Accounting
RFC 2178	OSPF MD5 cryptographic authentication / OSPFv2
RFC 2236	IGMPv2 for snooping
RFC 2270	BGP-4 Dedicated AS for sites/single provide
RFC 2328	OSPFv2
RFC 2338	VRRP: Virtual Redundancy Router Protocol
RFC 2362	PIM-SM
RFC 2385	BGP-4 MD5 authentication
RFC 2439	BGP-4 Route Flap Dampening
RFC 2453	RIPv2 Protocol
RFC 2460	IPv6 base stack
RFC 2464	Transmission of IPv6 packets over Ethernet networks
RFC 2545 and RFC 4710	IPv6 capable BGPv4+
RFC 2616	IPv6 HTTP server
RFC 2710 and RFC 3810	MLD (host-mode only)
RFC 2740	OSPFv3
RFC 2796	BGP Route Reflection – An Alternative to Full Mesh IBGP
RFC 2819	RMON
RFC 2874	DNS Extensions for IPv6
RFC 2918	Route Refresh Capability for BGP-4
RFC 2992	Analysis of an Equal-Cost Multi-Path Algorithm
RFC 3046	DHCP Option 82
RFC 3065	Autonomous System Confederations for BGP
RFC 3162	IPv6 RADIUS client
RFC 3315	IPv6 DHCP Relay

Request for comment	Description
RFC 3376	Internet Group Management Protocol, v3
RFC 3411 and RFC 2418	SNMP over IPv6 networks
RFC 3513	Internet Protocol Version 6 (IPv6) Addressing Architecture
RFC 3569	An overview of Source-Specific Multicast (SSM)
RFC 3587	IPv6 Global Unicast Address Format
RFC 3768 and draft-ietf-vrrp-ipv6-spec-08.txt	IPv6 capable VRRP
RFC 4213	IPv6 configured tunnel
RFC 4250–RFC 4256	SSH server and client support
RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC 4861	IPv6 Neighbor discovery
RFC 4862	IPv6 stateless address autoconfiguration
RFC 4893	BGP support for Four-octet AS Number Space
RFC 6329	IS-IS Extensions supporting Shortest Path Bridging

Quality of service

Table 24: Supported request for comments

Request for comment	Description
RFC 2474 and RFC 2475	DiffServ Support
RFC 2597	Assured Forwarding PHB Group
RFC 2598	An Expedited Forwarding PHB

Network management

Table 25: Supported request for comments

Request for comment	Description
RFC 959	File Transfer Protocol
RFC 1155	SMI
RFC 1157	SNMP
RFC 1215	Convention for defining traps for use with the SNMP
RFC 1258	BSD Rlogin
RFC 1269	Definitions of Managed Objects for the Border Gateway Protocol: v3
RFC 1271	Remote Network Monitoring Management Information Base
RFC 1305	Network Time Protocol v3 Specification, Implementation and Analysis3
RFC 1350	The TFTP Protocol (Revision 2)
RFC 1354	IP Forwarding Table MIB
RFC 1389	RIP v2 MIB Extensions
RFC 1757	Remote Network Monitoring Management Information Base
RFC 1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1908	Coexistence between v1 & v2 of the Internet-standard Network Management Framework
RFC 1930	Guidelines for creation, selection, and registration of an Autonomous System (AS)
RFC 2428	FTP Extensions for IPv6
RFC 2541	Secure Shell Protocol Architecture
RFC 2571	An Architecture for Describing SNMP Management Frameworks
RFC 2572	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)

Request for comment	Description
RFC 2573	SNMP Applications
RFC 2574	User-based Security Model (USM) for v3 of the Simple Network Management Protocol (SNMPv3)
RFC 2575	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 2576	Coexistence between v1, v2, & v3 of the Internet standard Network Management Framework
RFC 2616	IPv6 HTTP server
RFC 2819	Remote Network Monitoring Management Information Base
RFC 4250	SSH Protocol Assigned Numbers
RFC 4251	SSH Protocol Architecture
RFC 4252	SSH Authentication Protocol
RFC 4253	SSH Transport Layer Protocol
RFC 4254	SSH Connection Protocol
RFC 4255	DNS to Securely Publish SSH Key Fingerprints
RFC 4256	Generic Message Exchange Authentication for SSH

MIBs

Table 26: Supported request for comments

Request for comment	Description
RFC 1156	MIB for network management of TCP/IP
RFC 1212	Concise MIB definitions
RFC 1213	TCP/IP Management Information Base
RFC 1354	IP Forwarding Table MIB
RFC 1389	RIP v2 MIB Extensions
RFC 1398	Ethernet MIB

Request for comment	Description
RFC 1442	Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1450	Management Information Base for v2 of the Simple Network Management Protocol (SNMPv2)
RFC 1573	Interface MIB
RFC 1650	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 1657	BGP-4 MIB using SMIv2
RFC 1724	RIPv2 MIB extensions
RFC 1850	OSPF MIB
RFC 2096	IP Forwarding Table MIB
RFC 2452	IPv6 MIB: TCP MIB
RFC 2454	IPv6 MIB: UDP MIB
RFC 2466	IPv6 MIB: ICMPv6 Group
RFC 2578	Structure of Management Information v2 (SMIv2)
RFC 2674	Bridges with Traffic MIB
RFC 2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC 2863	Interface Group MIB
RFC 2925	Remote Ping, Traceroute & Lookup Operations MIB
RFC 2932	IPv4 Multicast Routing MIB
RFC 2933	IGMP MIB
RFC 2934	PIM MIB
RFC 3416	v2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC 4113	Management Information Base for the User Datagram Protocol (UDP)

Standard MIBs

The following table details the standard MIBs that Avaya Virtual Services Platform 9000 supports.

Table 27: Supported MIBs

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
STDMIB2— Link Aggregation Control Protocol (LACP) (802.3ad)	802.3ad	ieee802-lag.mib
STDMIB3—Exensible Authentication Protocol Over Local Area Networks (EAPoL) (802.1x)	802.1x	ieee8021x.mib
STDMIB4—Internet Assigned Numbers Authority (IANA) Interface Type	—	iana_if_type.mib
STDMIB5—Structure of Management Information (SMI)	RFC1155	rfc1155.mib
STDMIB6—Simple Network Management Protocol (SNMP)	RFC1157	rfc1157.mib
STDMIB7—MIB for network management of Transfer Control Protocol/Internet Protocol (TCP/IP) based Internet MIB2	RFC1213	rfc1213.mib
STDMIB8—A convention for defining traps for use with SNMP	RFC1215	rfc1215.mib
STDMIB9—Routing Information Protocol (RIP) version 2 MIB extensions	RFC1389	rfc1389.mib
STDMIB10—Definitions of Managed Objects for Bridges	RFC1493	rfc1493.mib

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
STD MIB11—Evolution of the Interface Groups for MIB2	RFC2863	rfc2863.mib
STD MIB12—Definitions of Managed Objects for the Ethernet-like Interface Types	RFC1643	rfc1643.mib
STD MIB13—Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2	RFC1657	rfc1657.mib
STD MIB14—RIP version 2 MIB extensions	RFC1724	rfc1724.mib
STD MIB15—Remote Network Monitoring (RMON)	RFC2819	rfc2819.mib
STD MIB16—Open Shortest Path First (OSPF) Version 2	RFC1850	rfc1850.mib
STD MIB17—Management Information Base of the Simple Network Management Protocol version 2 (SNMPv2)	RFC1907	rfc1907.mib
STD MIB21—Interfaces Group MIB using SMIv2	RFC2233	rfc2233.mib
STD MIB26a—An Architecture for Describing SNMP Management Frameworks	RFC2571	rfc2571.mib
STD MIB26b—Message Processing and Dispatching for the SNMP	RFC2572	rfc2572.mib
STD MIB26c—SNMP Applications	RFC2573	rfc2573.mib
STD MIB26d—User-based Security Model (USM) for version 3 of the SNMP	RFC2574	rfc2574.mib
STD MIB26e—View-based Access Control Model (VACM) for the SNMP	RFC2575	rfc2575.mib

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
STDMIB26f —Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework	RFC2576	rfc2576.mib
STDMIB29—Definitions of Managed Objects for the Virtual Router Redundancy Protocol	RFC2787	rfc2787.mib
STDMIB31—Textual Conventions for Internet Network Addresses	RFC2851	rfc2851.mib
STDMIB32—The Interface Group MIB	RFC2863	rfc2863.mib
STDMIB33—Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations	RFC2925	rfc2925.mib
STDMIB34—IPv4 Multicast Routing MIB	RFC2932	rfc2932.mib
STDMIB35—Internet Group Management Protocol MIB	RFC2933	rfc2933.mib
STDMIB36—Protocol Independent Multicast MIB for IPv4	RFC2934, RFC2936	rfc2934.mib, rfc2936.mib
STDMIB38—SNMPv3 These Request For Comments (RFC) make some previously named RFCs obsolete	RFC3411, RFC3412, RFC3413, RFC3414, RFC3415	rfc2571.mib, rfc2572.mib, rfc2573.mib, rfc2574.mib, rfc2575.mib
STDMIB39—Entity Sensor Management Information Base	RFC3433	
STDMIB40—The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model	RFC3826	rfc3826.mib
STDMIB41—Management Information Base for the	RFC4022	rfc4022.mib

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
Transmission Control protocol (TCP)		
STDNIB43—Management Information Base for the User Datagram Protocol (UDP)	RFC4113	rfc4113.mib
STDNIB44—Entity MIB	RFC4133	rfc4133.mib
STDNIB46—Definitions of Managed Objects for BGP-4	RFC4273	rfc4273.mib

Proprietary MIBs

The following table details the proprietary MIBs that Avaya Virtual Services Platform 9000 supports.

Table 28: Proprietary MIBs

Proprietary MIB name	File name
PROMIB1 - Rapid City MIB	rapid_city.mib
PROMIB 2 - SynOptics Root MIB	synro.mib
PROMIB3 - Other SynOptics definitions	s5114roo.mib
PROMIB4 - Other SynOptics definitions	s5tcs112.mib
PROMIB5 - Other SynOptics definitions	s5emt103.mib
PROMIB6 - Avaya RSTP/MSTP proprietary MIBs	nrrst000.mib, nnmst000.mib
PROMIB7 - Avaya IGMP MIB	rfc_igmp.mib
PROMIB8 - MIAvaya IP Multicast MIB	ipmroute_rcc.mib
PROMIB9 - Avaya PIM MIB	pim-rcc.mib
PROMIB11 - Avaya MIB definitions	wf_com.mib

Chapter 6: 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

The following sections identify the known issues in this release of the Avaya Virtual Services Platform 9000.

Alarm, logging, and error reporting

Table 29: Known issues

Issue number	Description	Workaround
wi00519967	Log filtering based on date and time is currently unavailable.	—
wi00980601	Enabling tracing to log can affect system performance in scaled environments.	Avaya recommends that you capture tracing by using a Telnet session, and capture to a file on the local management system to avoid potential performance issues. Verify that boot config flags trace-logging is not present in the configuration file to assure this feature is not enabled before you enable tracing.
wi00986085	After a CP switch-over the following message can appear in the logs: <code>smltTick: Initial MAC/ARP tbl completed, unlocked SMLT/SLT ports. The SMLT/SLT ports were not locked during the switch-over.</code> This	—

Known issues and limitations

Issue number	Description	Workaround
	message is incorrectly reused in this situation.	
wi01004076	<p>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</p>	This message has no functional impact and can be ignored.
wi01057618	<p>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 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</p>	These messages do not impact the operation of the switch and can be ignored.

Issue number	Description	Workaround
	<pre>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:rspRe ad32() k2b_pci_read failed rc: -1!!, k2DevId: 6, k2Slice: 2</pre>	
wi01092935	<p>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.</p>	This causes no negative issue.
wi01131833	<p>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.</p>	—

Applications

Table 30: Known issues

Issue number	Description	Workaround
wi00940744	The command show application vsptalk	View this information in the log file.

Issue number	Description	Workaround
	<code>client</code> does not show connection status.	

Chassis operations

Table 31: 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 <code>/usb</code> 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.
wi00930215	After you use the <code>extflash-stop</code> command to unmount the external Compact Flash, you must remove and reinsert the Compact Flash to remount the volume.	—
wi00969922	If you remove the backup CP module, you can see the following output on the console: <pre>fbuf allocated in "/vob/cb/nd_platform/ chassis/lib/ch_sync.c" at line 341 is freed</pre> 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.

Issue number	Description	Workaround
wi00970236	<p>The default value for the loadingconfig time is 15 minutes. The configurable range for the boot config loadconfigtime command is 0 to 300 seconds.</p> <p>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.</p> <p>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.</p>	—
wi01091558	<p>When using the Lifecycle menu to boot a new release, the following Lifecycle Error may be seen:</p> <pre>LifeCycle: ERROR: Can not get create /opt/patch link patch.</pre>	This message has no functional impact and can be ignored.
wi01096199	<p>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.</p>	Make sure all modules are up and operational, and then source the configuration file.
wi01123043 and wi01127303	<p>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</p>	—

Issue number	Description	Workaround
	up, nor does it have any effect on the boot-up.	
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.	An example workaround would be to use two separate static routes in the MgmtVRF: 134.0.0.0 255.0.0.0 135.0.0.0 255.0.0.0 so you will not need to use a less than 8 bit mask.
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.	This sensor is not relevant for the thermal health of the I/O blade as it measures the temperature of the inflow of air into the chassis and not a measure of cooling across the I/O blade. A better gauge of thermal behavior is to use I/O sensor 1, which is optimally positioned to measure the cooling across the blade.
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.

COM

Table 32: Known issues

Issue number	Description	Workaround
—	COM support is not available for the initial release of Virtual Services Platform 9010.	COM support for Virtual Services Platform 9010 will be available in COM Release 3.1.
wi01130603	In COM, the EDM Plugins Inventory does not display the SVN Revision Number of the plugin.	The only way to view the SVN is to launch Element Manager, and see it at the bottom of the screen, inside the Element Manager window.

EDM
Table 33: Known issues

Issue number	Description	Workaround
wi00830411	Error messages may be displayed on the console when connected to EDM using Internet Explorer 6.0. Internet Explorer 6.0 is not supported.	Discontinuing use of this browser will discontinue the error messages.
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.	—

Issue number	Description	Workaround
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.	—
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.	—
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 RsmIteEnable field displays the correct status for the VLAN.	Use ACLI or the Configuration > IPv6 > IPv6 > Interfaces navigation path in EDM.
wi01152214	Cannot access EDM using Firefox version 27.	Do not upgrade Firefox to version 27. Continue to use Firefox version 26.

HA operations

Table 34: Known issues

Issue number	Description	Workaround
wi00937861	The exception dump max-disk-space configuration	—

Issue number	Description	Workaround
	ACL command is not available on the standby CPU.	
wi01106991	<p>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:</p> <pre>SW WARNING smltProcLearnMacAddrW ithLifidVRRP 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 smltDumpLearnMacAddrL ifidMsgmac 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</pre> <p>After configuration, all 255 VRRP interfaces are UP on both IST peer switches.</p>	This warning appears due to an occasional race condition while configuring VRRP. There is no traffic loss, service impact, or side effects.

Hardware

Table 35: 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	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 <i>Avaya Virtual Services</i>

Issue number	Description	Workaround
	insertion lever does not catch the gasket.	<i>Platform 9000 Installation — Modules</i> , NN46250-301.

Management and general administration

Table 36: 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.
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 <i>Avaya Virtual</i>

Issue number	Description	Workaround
		<p><i>Services Platform 9000 Configuration — IP Routing, NN46250-505.</i></p> <p>If by mistake you do get into this situation, on the host where you initiate FTP, set FTP to passive.</p>
wi01129311	<p>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.</p>	<p>If the mirrored packets must go out on 3/1, use the out-port parameter.</p>
wi01131449	<p>The device can display the following messages when an invalid MIB GET request occurs for non-existent ports.</p> <pre data-bbox="558 856 938 982">IO5 [09/05/13 03:30:48.655] 0x0011052a 00000000 GlobalRouter COP- SW ERROR lcdPimPortToMac: invalid PIM_PORT[63]</pre> <pre data-bbox="558 1003 938 1150">IO5 [09/05/13 03:30:48.655] 0x0011052a 00000000 GlobalRouter COP- SW ERROR lcdPimPortToMacPort: invalid PIM_PORT[63]</pre> <pre data-bbox="558 1171 938 1318">IO5 [09/05/13 03:30:48.655] 0x0025c554 00000000 GlobalRouter COP- SW ERROR cb_sw_port_get_stats error: wrong unit[4]</pre>	<p>Does not impact service.</p>
wi01137524	<p>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.</p>	<p>Do not configure the CP limit higher than slot 8.</p>

MLT, SMLT, and link aggregation

Table 37: Known issues

Issue number	Description	Workaround
wi00822560	Disable member ports before deleting an MLT.	—
wi00822571	In rare occurrences traffic loops can be introduced if ports are removed from and MLT before being disabled.	The operator must disable participating ports before removing them from the MLT, or deleting the MLT completely.
wi01097311	<p>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.</p> <p>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.</p> <p>A lane refers to the following grouping of ports on an interface module:</p> <ul style="list-style-type: none"> • 9024XL: a group of four ports, for example 1-4 or 5-8, and so on. • 9048GB or 9048GT: a group of eight ports, for example, 1-8 or 9-16, and so on. 	Do not mix LACP and static MLT ports within the same group of ports that comprise a lane.

Multicast

Table 38: Known issues

Issue number	Description	Workaround
—	The ACLI query-interval parameter for PIM interfaces and ports is changed to hello-interval. You can still use the query-interval parameter, but the configuration file saves this information as hello-interval and query-interval does not appear in ACLI Help text.	—
—	<p>If you need to upgrade the IGMP version of routers in a network that operates using a lower version of IGMP (caused by the dynamic downgrade function), perform the following actions on all routers:</p> <ol style="list-style-type: none"> 1. Disable PIM on the interface on which you need to upgrade the IGMP version. 2. Change the IGMP version to the required value. 3. Enable PIM on the interface you just upgraded. 	—
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.	<p>This issue has 3 workaround scenarios:</p> <ol style="list-style-type: none"> 1. IGMP V2 SSM range membership reports are fully supported on Layer 3 VSN Multicast interfaces by configuring the interface as follows: <ol style="list-style-type: none"> a. Set the IGMP version of the Layer 3 VSN multicast interface to 3.

Issue number	Description	Workaround
		<p>b. Enable <code>ip igmp compatibility-mode</code>.</p> <p>2. The IGMP SSM range on the VRF is configurable and can be configured to restrict the SSM range to just one unused 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.</p> <p>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:</p> <pre>(config-if)#ip igmp static-group 232.1.1.1 232.1.1.2 6/1 static</pre>

Patching and upgrading

Table 39: Known issues

Issue number	Description	Workaround
wi00511642	The <code>software patch commit</code> and <code>software patch remove</code> commands will not display messages such as Syncing release directory on backup CP card in slot 2 while	—

Issue number	Description	Workaround
	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 patches were applied, even though they were.	Use the show software patch command to see the status of the patches.
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.

Routing

Table 40: Known issues

Issue number	Description	Workaround
wi01140262	BGP peer groups for VRFs are not saved correctly in the configuration file. The <code>ip bgp</code>	—

Issue number	Description	Workaround
	statement is missing from the configuration file.	
wi01145272	Virtual Router Redundancy Protocol (VRRP) not working on Network-to-Network Interface (NNI).	—
wi00974143	You cannot change the OSPF area for an IPv6 interface. You must delete the interface from one OSPF area, and then create the new OSPF area.	—
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: <ol style="list-style-type: none"> 1. Obtain show ip ospf ase information from both Master and Standby CPs. 2. Compare output: <ol style="list-style-type: none"> 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	This condition is a misconfiguration in the network and very rare. If this condition occurs, enable tracing for OSPF to see the trace

Issue number	Description	Workaround
	<p>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.</p> <p>These framework sync errors indicate a problem syncing the duplicate Router ID 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.</p>	<p>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.</p>
wi01122597	<p>show ip arp does not show the total number of ARP entries for the current VRF.</p>	<p>If you want to see an ARP summary per VRF, including the current VRF, use show ip vrf.</p>
wi01126460	<p>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 address 2000::1 may be reachable with a more specific route.</p>	<p>Always configure static routes with a link-local next hop instead of global.</p>
wi01140262	<p>BGP peer groups for VRFs are not saved correctly.</p>	<p>Edit the config.cfg file, and add <code>ip bgp before neighbor <peer-group> enable</code>.</p>
wi01141461	<p>The IPv6 filtering functionality is not supported and should not be used even though the ACLI commands are visible. Virtual Services Platform 9000 does not support the following IPv6 filters:</p>	<p>Do not use these commands. Virtual Services Platform 9000 does not support IPv6 filters in this release.</p>

Issue number	Description	Workaround
	<ol style="list-style-type: none"> 1. The packet type filter in the filter acl type command. 2. The IPv6 filter in the filter acl ace command. 3. The IPv6 filter in the show filter acl command. <p>These commands will be removed in Release 3.4.1.</p>	

SPBM and IS-IS

Table 41: Known issues

Issue number	Description	Workaround
wi01004034	The ERS show isis spbm show-all command is not available on VSP 9000.	
wi01109764	<p>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:</p> <pre> 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 </pre>	<p>Disable and re-enable IGMP snooping. Perform the following in ACLI:</p> <pre> # config terminal (config)# interface vlan 100 (config-if)# no ip igmp snooping (config-if)# ip igmp snooping </pre>

Issue number	Description	Workaround
	<pre>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</pre>	
wi01117073	<pre>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.</pre>	There is no functional impact observed.
wi01117528	Abnormal shutdown seen when CFM C-MAC 12 traceroute <A.B.C.D> runs.	—
wi01128615	When a VSP 9000 receives MinM packets with a Destination MAC as that of its own B-MAC, ingress mirroring on NNI ports will show the B-TAG ethertype as 0x88A8 even if 0x8100 was used on the wire.	—
wi01137529	Newly created VLANs with VRFs and I-SIDs do not have the routing bit set.	Configure the IP address on the C-VLAN prior to adding the ports to the C-VLAN.
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	Add the port to the MLT before you enable IS-IS on the MLT.

Issue number	Description	Workaround
	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.	Reconfigure the route metric after the route-policy is disabled.
wi01141033	A discovered I-SID may be labelled incorrectly as type local.	—
wi01151658	IS-IS adjacencies are brought down (deleted) before their hold-down time expire, which results in unnecessary flapping within the SPB network.	To recover from this situation, disable and enable IS-IS on the node experiencing the problem.

Interoperability issues

The following table lists the known issues between this release of the Avaya Virtual Services Platform 9000 and other Avaya products. The following table also identifies if the issue is fixed in a specific release. Note that the issue will still exist in previous releases.

Table 42: Interoperability issues

Issue number	Description	Workaround	Fixed in release
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.	—	ERS 8600 5.1.7.0
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 8600 to remove the loop.	ERS 8600 5.1.8.0
wi00689238	If a VSP 9000 aggregation switch sends a high	—	ERS 8600 5.1.6.0

Issue number	Description	Workaround	Fixed in release
	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).	—	ERS 8600 5.1.4.0
wi01099098	You cannot use CFM between VSP 9000 and ERS 8800 to perform an I2 ping or I2 traceroute for a C-MAC.	—	ERS 8800 7.2.1.1 VSP 9000 3.4

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 43: Limitations and expected behaviors

Issue number	Description	Workaround
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.
wi00664833	The MAC DA filter only applies for traffic that is bridged through the device. If the packet is routed, then the legacy MAC DA filter does not apply for traffic that is routed through the box.	Use ACL-based filters to implement the MAC DA filter. The ACL-based filter works correctly regardless of whether the packet is bridged or routed.
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.
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	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

Issue number	Description	Workaround
	<p>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.</p> <p>You may need to configure timers proportionately to the anticipated multicast route load.</p>	<p>by multicast scaling considerations.</p>
wi00981875	<p>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.</p>	<p>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.</p>
wi01068569	<p>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.</p> <p>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.</p>	—
wi01086118	<p>Ingress port mirroring does not work if the VLAN for the incoming packet does not match the VLAN for the port.</p>	—

Chapter 7: Resolved issues in Release 3.4.0.2, Release 3.4.0.1, and Release 3.4.0.0

This chapter identifies the issues resolved in Release 3.4.0.2, Release 3.4.0.1, and Release 3.4.0.0.

Resolved issues in Release 3.4.0.2

This section identifies the issues resolved in Release 3.4.0.2

Application connectivity issue

Table 44: Resolved issue

Issue number	Issue description																
wi01140900	<p>Application connectivity issues with the following log message observed.</p> <pre>COP-SW ERROR K2-0 Zag-1 PMM Error Ext Adr = 0x1010, Data = 0x80010000</pre> <p>Frame Error and Exception drops incrementing in the show khi forwarding rsp output.</p> <pre>VSP-9012:1#show khi forwarding rsp 5</pre> <p>[data omitted for brevity]</p> <hr/> <table><thead><tr><th>Health Indicator</th><th>Ports 5-8</th><th>Ports 13-16</th><th>Ports 21-24</th></tr></thead><tbody><tr><td>LSM Drops</td><td>3862420</td><td>3863299</td><td>3863454</td></tr><tr><td>Exception Drops</td><td>478</td><td>0</td><td>0</td></tr><tr><td>Frame Error Drops</td><td>472</td><td>0</td><td>0</td></tr></tbody></table>	Health Indicator	Ports 5-8	Ports 13-16	Ports 21-24	LSM Drops	3862420	3863299	3863454	Exception Drops	478	0	0	Frame Error Drops	472	0	0
Health Indicator	Ports 5-8	Ports 13-16	Ports 21-24														
LSM Drops	3862420	3863299	3863454														
Exception Drops	478	0	0														
Frame Error Drops	472	0	0														

Failed RSP Microcode ERROR

Table 45: Resolved issue

Issue number	Issue description
wi01143196	Failed RSP Microcode ERROR resulted in invalid Split MultiLink Trunking (SMLT) forwarding.

IP redirect next-hop filter

Table 46: Resolved issue

Issue number	Issue description
wi01133761	IP redirect next-hop filter was not remarking the ingress DSCP value or dot1q correctly at the egress.

High Availability with CFM C-MAC

Table 47: Resolved issue

Issue number	Issue description
wi01147016	On a Virtual Services Platform 9000 running in high availability mode with CFM CMAC, if you delete and re-add a VLAN this can cause the secondary CP module to reset.

Resolved issues in Release 3.4.0.1

This section identifies the issues resolved in Release 3.4.0.1.

Routing

Table 48: Resolved issues

Issue number	Issue description
wi01136486	There may be an issue with receiving ICMP echo responses from the VRRP IP address when pinging this address through the VRRP node that is in a 'backup' state.

Resolved issues in Release 3.4.0.0

This section identifies the issues resolved in Release 3.4.0.0.

Alarm, logging, and error reporting

Table 49: Resolved issues

Issue number	Issue description
wi00768362	The show alarm database command does not show the CPU from which the alarm originated. The log report contains this information.

Applications

Table 50: Resolved issues

Issue number	Issue description
wi01002102	ACLI does not enforce the VSP Talk restriction of no all-numeric passwords.
wi01002448	Deleting VSP Talk does not disable the messaging to the client.

COM

Table 51: Resolved issues

Issue number	Issue description
wi00949006	You cannot view more than 50 ARP entries using COM.

EDM

Table 52: Resolved issues

Issue number	Issue description
wi00668629	After deleting a VRF, all open EDM sessions that are using that VRF need to be closed manually by the user.
wi00962229	EDM does not show the TTL field in the ARP table.
wi00968931	You cannot configure EDM to use an IPv6 address for the Help directory on a TFTP server.
wi00969780	EDM does not show the tunnel field in the ARP table.
wi00994286	EDM does not support cross VRF route redistribution. You can use only the current VRF context as the destination and source VRF, and you can use only the route policies you create under the current VRF context. For example, if you use VRF1 as the VRF context, the destination and source VRF is VRF1. For route redistribution, you can use only policies created under the VRF1 context.
wi01004052	EDM does not support the <code>/intflash</code> , <code>/extflash</code> , or <code>/usb</code> path options for the EDM Help files.

Hardware

Table 53: Resolved issues

Issue number	Issue description
wi01005012	If you hot insert an SFP or SFP+ into a 9024XL or 9048GB module, the port is erroneously enabled even if the port is administratively disabled. The LED changes to solid amber, which indicates the port is enabled, or solid green if it connects to a live port.
wi01006381	A port can go into the blocking state if you change its configuration while the interface module to which it belongs is not present, for example, is removed or powered down.

Management and general administration

Table 54: Resolved issues

Issue number	Issue description
wi00932777	The current release does not support IPv6 addresses for the traceroute command.
wi01002533	Executing a MIB walk on the proprietary Routing Table MIB .1.3.6.1.4.1.2272.1.8.7 when alternative routes are present, and the alternative route nexthop is less than the best route nexthop, will fail.
wi01047358	The minimum datasize for Ping packets must increase. The maximum length for Traceroute packets must decrease.
wi01068232	The show sys action command has no function for Virtual Services Platform 9000 and provides invalid output.
wi01069397, wi01069407, wi01069414	Three issues exist related to SNMP-server community configuration: <ul style="list-style-type: none"> • The system does not require you to create a new group name if you use a new

Issue number	Issue description
	<p>security name to create an SNMP-server community. You must create a new group name.</p> <ul style="list-style-type: none"> • The system requires you to create a new group name if you use a default security name to create an SNMP-server community. You do not need to create a new group name in this situation. • The system allows a space in the group name. This space breaks the relationship between the view and the group associated with that view.
wi01072700	The system indicates the SSH port range can support a port number greater than 49151. 49151 is the upper limit for the port range.
wi01082535	The system indicates the minimum port value for the Traceroute UDP range can be zero (0). The lower limit value is one (1).

Patching and upgrading

Table 55: Resolved issues

Issue number	Issue description
wi00989121	When you upgrade the software image, a slight chance exists that one of the Switch Fabric or interface modules can fail to upgrade, which results in a rollback to the previous release.
wi00990115	The console can display error messages when you revert a patch.
wi01007353	Modules with factory images do not upgrade if the CP module in slot 2 is the master and the CP module in slot 1 is not operational.

Routing

Table 56: Resolved issues

Issue number	Issue description
wi00703966	There is a problem that can cause the standby CP to reboot during the synchronization of a large number of BGP routes from the master CP. If this does occur, the standby CP will reboot and attempt to synchronize with the master CP again. It will very likely synchronize correctly on the second attempt. During the time of standby CP reboot and resynchronization the traffic flow through the system is not effected because the master CP stays operational.
wi01014704	The show ip route ACLI command shows incorrect routing protocols for inter-VRF redistributed routes. This issue is a display issue only, and does not have functional impact on inter-VRF route redistribution.

SPBM and IS-IS

Table 57: Resolved issues

Issue number	Issue description
wi01000756	Removing a 9024XL module that was configured for IS-IS/SPBM does not properly remove all IS-IS configuration. This situation is not an issue if you replace the module with another 9024XL module.

VLAN operations

Table 58: Resolved issues

Issue number	Issue description
wi01005885	If you configure NLB unicast mode, you can ping the NLB cluster address, but cannot ping the physical server address.