Release Notes — Release 3.2
Avaya Virtual Services Platform 9000

3.2
NN46250-401
03.06
October 2012

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

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

Heritage Nortel Software

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

Copyright

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

Third-party components

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

Preventing Toll Fraud

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

Avaya Toll Fraud Intervention

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

Trademarks

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Purpose of this document

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.

Chapter 2: New in this release

The following sections detail what's new in *Avaya Virtual Services Platform 9000 Release Notes* (NN46250–401) for Release 3.2.

Features

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

Hardware support

Beginning with Release 3.2, you can hot swap the following items:

- multiple modules simultaneously
- the external Compact Flash on the CP module

For more information, see Supported hardware on page 12 and Removing external storage devices from the CP module on page 19.

New features

This release provides or enhances support for the following features:

- BGP 4–byte AS
- IGMPv3
- IPv6
- Log messages
- Lossless Ethernet
- VLANs on Link Aggregation Control Protocol (LACP) ports
- VSP Talk

For more information, see the following sections:

- New features on page 11
- Supported RFCs on page 38
- Software scaling capabilities on page 32

Other changes

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

Introduction

The Introduction chapter is renamed to Purpose of this document on page 7 and moved to the beginning of the document.

EDM Help

EDM Help does not open for every tab in Release 3.2. For more information, see EDM Help on page 26.

Known issues

Known issues on page 53 is updated.

Resetting multiple modules

Resetting multiple modules on page 23 is added to the document.

Resolved issues

Resolved issues on page 69 is updated for issues fixed 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

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

BGP 4–byte AS

Release 3.2 supports 4–byte AS numbers as the pool of assigned 2–byte AS numbers will soon be exhausted. For more information, see *Avaya Virtual Services Platform 9000 Configuration — BGP Services*, NN46250–507.

IGMPv3

Release 3.2 enhances IGMPv3 support to be fully compliant with RFC3376. The enhancements affect the filter modes of include and exclude. You can now configure multiple sources for the same group in the ssm-map. IGMPv3 and PIM-SM can function together. For more information, see *Avaya Virtual Services Platform 9000 Configuration — IP Multicast Routing Protocols*, NN46250–504.

IPv6

Release 3.2 introduces support for IPv6 routing. The IPv6 implementation includes support for OSPFv3, VRRP, RSMLT, and BGP+. For more information, see *Avaya Virtual Services Platform 9000 Configuration — IPv6 Routing*, NN46250–509, *Avaya Virtual Services Platform 9000 Configuration — BGP Services*, NN46250–507, and *Avaya Virtual Services Platform 9000 Commands Reference — ACLI*, NN46250–104.

Log messages

Prior to Release 3.2, the system stored the CLI log and SNMP log in two separate files on the external flash: clilog.txt and snmplog.txt. The system did not send the SNMP log to the syslog server. Beginning with Release 3.2, CLI log messages and SNMP log (set) messages are included in the main system log file, which can be sent to an external syslog server. New options are added to the **`show logging file module`** command to view just the CLI log or SNMP log messages. You can still use **`show <clilog|snmplog> file`** and **`save <clilog|snmplog> file`** commands for files created prior to Release 3.2.

Also in Release 3.2, the format of module identification in log messages is updated. Prior to Release 3.2, the log message identified which CP module logged the message, and the slot number of the affected module was embedded later. In the following example, the beginning of the old format log message identifies CPU1, and the module in slot 5 is identified later.

```
CPU1 [08/17/10 11:38:04.875] 0x0009059e 00000000 GlobalRouter QOS
INFO Slot 5: QOS profile set to 0
```

The following example shows the new log message format that identifies the module at the beginning of the message text:

```
IO5 [08/17/11 11:38:04.875] 0x0009059e 00000000 GlobalRouter QOS INFO
QOS profile set to 0
```

For more information about logging and log messages, see *Avaya Virtual Services Platform 9000 Troubleshooting*, NN46250–700.

Lossless Ethernet

Beginning with Release 3.2, you can configure 10 GbE Ethernet ports with SFP+ connectors to be lossless.

Avaya recommends that you do not enable tx-flow control on a lossless port. If you enable tx-flow control on a lossless port, Avaya cannot guarantee appropriate lossless behavior

For more information, see *Avaya Virtual Services Platform 9000 Planning and Engineering — Network Design*, NN46250–200 and *Avaya Virtual Services Platform 9000 Configuration — Ethernet Modules*, NN46250–508.

VLANs on Link Aggregation Control Protocol (LACP) ports

You can now dynamically add or remove VLANs on LACP ports. For more information, see *Avaya Virtual Services Platform 9000 Configuration — Link Aggregation, MLT, and SMLT*, NN46250–503.

VSP Talk

Release 3.2 introduces a new feature, VSP Talk, that you can use to monitor the system from an instant messaging (IM) client. For more information, see *Avaya Virtual Services Platform 9000 Administration*, NN46250–600.

Supported hardware

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

New hardware

No new hardware is added for this release.

Prior to Release 3.2, you had to insert and configure one module at a time. Beginning with Release 3.2, you can hotswap multiple modules simultaneously.

9012 Chassis

The 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 Control Processor (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 Switch Fabric (SF) modules and two back slots are for future development. The two back bays are for SF cooling modules.

The following table details the weight and dimensions of the 9012 chassis.

Table 1: 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)
Weight (chassis, midplane, cooling modules, and filler panels)	288 lb (131 kg)

The 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 for lifting the 9012 chassis.

9006AC power supply

The 9006AC power supply accepts 100 to 120 volts alternating current (V AC) and 200 to 240 V AC input voltage using 20 amps (A) plugs and drawing approximately twelve A. With 100 to 120 V AC nominal input voltage conditions, the power supply produces a maximum of 1200 Watts of 48 volts direct current (V DC) power. With 200 to 240 V AC nominal input voltage conditions, the power supply can output 2000 Watts of 48 V DC power.

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 2: Supported external storage devices

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

Note:

Avaya recommends that you use the Avaya Compact Flash device (EC1411010-E6) with the VSP 9000 because it has been validated for proper operation on the VSP 9000. Avaya recommends that you 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 19.

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

- six for the power supplies
- six for the Switch Fabrics
- two for the auxiliary modules
- four for the fans
- one for the central processor 1 on the CP module
- one for the central processor 2 on the CP module
- one for the AUX processor on the CP module, for future use
- one for master
- one for system temperature

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 18. Failure to follow this procedure can result in file system corruption.

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.

9090SF Switch Fabric module

The 9090SF Switch Fabric (SF) modules provide the back end switching solution in the midplane 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 8.5 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 3: Switch Fabric 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. The 9048 modules have a throughput capability of 70 Mpps.

9012SC Switch Fabric cooling module

The 9012SC SF cooling modules contain two fans each to cool the SF modules. You install them in the back of the chassis.

9012FC IO cooling module

The 9012FC IO cooling modules contain eight fans each to cool the interface modules. You install them from the front of the chassis.

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 supports a maximum throughput of 105

Mpps over 24 ports of 10 Gb/s Ethernet traffic using standard SFP+ fiber connectors. The module supports SR, LR, LRM, and ER SFP+ format.

The following table details the multimode fiber (MMF) and single-mode fiber (SMF) SFP and SFP+ fiber connectors supported by the 9024XL module.

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

Model number	Product number	Description
10GBASE-SR/SW	AA1403015-E6	850 nanometers (nm). The range is up to the following: • 22 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, 500 MHz-km MMF • 82 m using 50 µm, 500 MHz-km MMF • 300 m using 50 µm, 2000 MHz-km MMF
10GBASE-LRM	AA1403017-E6	1310 nm. Up to 220 m reach over Fiber Distributed Data Interface (FDDI)-grade 62.5 µm multimode fiber. Suited for campus LANs.
10GBASE-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-CX	AA1403018-E6 to AA1403021-E6	4-pair twinaxial copper cable to connect 10 Gb ports. The maximum range is 15 m.
1000BASE-SX	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	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.

Model number	Product number	Description
1000BASE-XD	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	AA1419052-E6	1550 nm (non-CWDM). The range is up to 70 km over SMF pair.
1000BASE CWDM	AA1419053-E6 to AA1419060-E6	1470 nm to 1610 nm (CWDM). The range is up to 40km over SMF pair.

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

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.

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 connectors supported by the 9048GB module.

Table 5: Supported SFP connectors 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	AA1419048-E6	850 nm, up to 275 or 550 m
1000BASE-LX	AA1419049-E6	1310 nm, up to 10 km
1000BASE-XD	AA1419050-E6	1310 nm, up to 40 km
	AA1419051-E6	1550 nm, up to 40km (non-CWDM)
1000BASE-ZX	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

Model	ROHS product number	Description
1000BASE-BX-D	AA1419070-E6	1490 nm, up to 10km
	AA1419077-E6	1490 nm, up to 40km
1000BASE-EX	AA1419071-E6	1550 nm, up to 120 km (non-CWDM)
1000BASE 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 100/1000M capable.

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

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. Log on to 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 have elapsed. This 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 VSP 9000 stop command will 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:

Avaya recommends that you use the Avaya Compact Flash device (EC1411010-E6) with the VSP 9000 because it has been validated for proper operation on the VSP 9000. Avaya recommends that you 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.

Procedure

1. 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.
2. 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 VSP 9000 automatically recognizes them. The devices are accessible within seconds after insertion.

After you insert the external Compact Flash, you should enable logging to the external Compact Flash by using 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. File sizes are approximate.

Table 6: Software files

File name	Description	Size
VSP9K.3.2.0.0.tgz	Release 3.2 archived distribution	97.2 MB
VSP9K.3.2.0.0_modules.tgz	Encryption modules	38 KB

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 7: Open Source software files

File name	Description	Size
VSP9K.3.2.0.0_oss-notice.html	Master copyright file. This file is located in the Licenses directory.	403 KB
VSP9K.3.2.0.0_OpenSource.zip	Open source base software for Virtual Services Platform 9000 Release 3.2.	310 MB

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

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.

Always place the modules on appropriate antistatic material.

Support the module from underneath with two hands. Do not touch the top of the module. Do not touch the pins or electrical connections.

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.

Be careful not to bump module connectors against the ejector levers of an adjacent module. Damage to connectors can result.

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 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 8.0
- Mozilla Firefox 7.x

Environmental specifications

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

Table 8: Minimum and maximum operational environmental specifications

Operating environmental specification	Min	Max
Temperature	0°C	60°C
Relative humidity	10%	90%
Altitude	0 ft	10 000 ft
Thermal Shock	-40C	85C

Operating environmental specification	Min	Max
Vibration, peak to peak displacement	—	0.005 in. (5 to 32 Hz)
Audible noise	—	60 DB

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

Table 9: Minimum and maximum storage environmental specifications

Storage environmental parameter	Min	Max
Temperature	-25°C	70°C
Relative Humidity	—	90%
Altitude	—	10 000 ft

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

Table 10: Unpackaged operational requirements

Unpackaged operational requirements	Standard specification	Note
Operational vibration (Sinusoidal)	European Telecommunications Standard (ETS) 300 019-1-3 and International Electrotechnical Commission (IEC) 68-2-6 test Fc	Shock of low significance, such as slamming door
Shock 30g 11ms	International Electrotechnical Commission (IEC) 68-2-27	Shock of low significance

The following table lists the requirements of an unpackaged Virtual Services Platform 9000 for storage and transport.

Table 11: Unpackaged nonoperational requirements

Unpackaged 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

Unpackaged nonoperational Requirements (Storage and transport)	Standard specification	Note
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 heigth of 75 cm.)	Bellcore GR-63-CORE issue 1 oct 1995	Transportation handling

Reliability

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

Table 12: Reliability

Component	Mean time between failures
Chassis	500,000 hours
Fan tray module	500,000 hours
Power supply module	1,500,000 hours
Switch Fabric module	1,447,178 hours
Control Processor module	777,001 hours
Interface modules	• 9024XL — 209,908 hours • 9048GB — 267,953 hours • 9048GT — 278,629 hours
Hard Drive and Auxiliary modules	200,000 hours

IPv6 addressing

Virtual Services Platform 9000 supports IPv6 addressing with 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

User configurable SSL certificates

Virtual Services Platform 9000 does not support user configurable SSL certificates.

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.

EDM Help

In Release 3.2, a number of EDM tabs do not open a Help page after you click the **Help** button. You can view this Help information by opening the EDM Help from another tab, and then navigating the **Contents** tab of the EDM Help. The following table identifies the EDM tab, the location within the EDM Help Contents, and the customer document that includes a relevant procedure and field descriptions for each tab.

EDM tab	EDM Help contents	Document	Procedure title
Edit > **Card** > **Storage Usage**	**Administration** > **Basic adminstration procedures using EDM**	*Avaya Virtual Services Platform 9000 Administration*, NN46250–600	Displaying available storage space
Edit > **Card** > **Flash Files**	**Administration** > **Basic adminstration procedures using EDM**	*Avaya Virtual Services Platform 9000 Administration*, NN46250–600	Displaying internal flash files for a CP module
Edit > **File System** > **Copy File**	**Administration** > **Basic adminstration procedures using EDM**	*Avaya Virtual Services Platform 9000 Administration*, NN46250–600	Copying a file
Edit > **File System** > **Device Info**	**Administration** > **Basic adminstration procedures using EDM**	*Avaya Virtual Services Platform 9000 Administration*, NN46250–600	Displaying storage use
Edit > **File System** > **Flash Files**	**Administration** > **Basic adminstration procedures using EDM**	*Avaya Virtual Services Platform 9000 Administration*, NN46250–600	Displaying flash file information
Edit > **File System** > **External Flash Files**	**Administration** > **Basic adminstration procedures using EDM**	*Avaya Virtual Services Platform 9000 Administration*, NN46250–600	Displaying external flash file information
Edit > **File System** > **USB Files**	**Administration** > **Basic adminstration procedures using EDM**	*Avaya Virtual Services Platform 9000 Administration*, NN46250–600	Displaying USB file information
Edit > **Port** > **General** > **Lossless Ethernet**	**Ethernet module configuration** > **Lossless Ethernet configuration using EDM**	*Avaya Virtual Services Platform 9000 Configuration — Ethernet Modules*, NN46250–508	Configuring Lossless Ethernet using EDM

The Help for the embedded-EDM (on device EDM) does not currently support the search function. Search functionality in the embedded-EDM Help will be added in a future release. The search function is supported for Help in the EDM plug-in for COM.

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 VSP 9000 Software Release 3.2 incorporates all fixes from prior releases, up to and including, Release 3.0.1.x patches and Release 3.1.1.0.

Hardware and software compatibility

The following tables describe the hardware and the minimum Avaya Virtual Services Platform 9000 software version required to support the hardware.

Table 13: Hardware and minimum software version

Chassis, switching fabrics, and control processors			Minimum software version	Part number
	9012VSP chassis	12-slot chassis	3.0	EC1402001-E6
	9090SF	Switch Fabric module	3.0	EC1404006-E6
	9080CP	Control Processor module	3.0	EC1404007-E6
Power Supplies				
	9006AC	1200–2000W AC Power Supply	3.0	EC1405A01-E6
Cooling modules				
	9012SC	Side Fan Tray	3.0	EC1411001-E6

Chassis, switching fabrics, and control processors			Minimum software version	Part number
	9012FC	Fabric Fan Tray	3.0	EC1411002-E6
Ethernet modules				
	9024XL	24-port 10GBASE-X SFP +/SFP	3.0	EC1404001-E6
	9048GB	48-port 1000BASE-X SFP	3.0	EC1404002-E6
	9048GT	48-port 10/100/1000BASE-T	3.0	EC1404003-E6
Compatible SFPs and SFP+s For more information about SFP and SFP+, see *Avaya Virtual Services Platform 9000 Installation — SFP Hardware Components, NN46250-305*				
	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		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.

Chassis, switching fabrics, and control processors			Minimum software version	Part number
	1000BASE DDI CWDM 70 km SFP	Gigabit Ethernet, duplex LC connector	3.0	AA1419061-E6 to AA1419068-E6.
	10GBASE-SR/SW SFP+	300m, 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-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

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 14: Hardware scaling capabilities

	Maximum number supported
9024XL I/O module	
10GbE fiber connections	240 (10 x 24)
Processor	1 GHz
9048GB I/O module	
GbE fiber connections	480 (10 x 48)
Processor	1 GHz
9048GT I/O module	
10/100/1000 copper connections	480 (10 x 48)
Processor	1 GHz
9080CP CP module	
Processor	1.33 GHz
Console port	1 D-subminiature 25-pin shell 9 pin connector (DB9) per CP module
Ethernet management	1 Registered Jack (RJ) 45 per CP module
USB port	1 Universal Serial Bus (USB) Type A (Master) per CP module
External Compact Flash	1 per CP module
9012 Chassis	

	Maximum number supported
Control Processor (CP) modules	2
Interface modules	10
Switch Fabric (SF) modules	6 You must install a minimum of 3 SF modules in the chassis.
Auxiliary slots	2
Power supplies	6
Total power capacity	• 10 kW in 220 V AC mode • 6 kW in 110 V AC mode
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 15: Software scaling capabilities

	Maximum number supported
Layer 2	
IEEE/Port-based VLANs	4,084
Inter-Switch Trunk (IST)	1 group
Internet Protocol (IP) Subnet-based VLANs	256
LACP	512 aggregators
LACP ports per aggregator	8 active and 8 standby
Lossless Ethernet	2 ports for each 8–port cluster 6 ports for each 9024XL module
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

	Maximum number supported
Source MAC-based VLANs	100
Split Multi-Link Trunking (SMLT)	511 groups
SMLT ports per group	16
VLACP Interfaces	128
Layer 3	
Address Resolution Protocol (ARP) for each port, VRF, or VLAN	64,000 entries total
BGP Internet peers (full)	3
BGP peers	256
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
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 (Brouter)	480
IP prefix entries	25 000
IPv4 prefix list	500
IP routing policies	500 for each VRF 5,000 for each system
IPFIX flows	96,000 for each interface module 960,000 for each chassis
IPv4 or IPv6 FTP sessions	4 each, 8 total
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

	Maximum number supported
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 source and group (S, G)	6,000
NLB Clusters — Multicast, with multicast MAC flooding disabled	1 for each VLAN 2,000 for each system
NLB Clusters — Multicast, with multicast MAC flooding enabled	128 for each VLAN 2,000 for each system
NLB Clusters — Unicast	128 for each VLAN 2,000 for each system
OSPF adjacencies	512
OSPF areas	12 for each OSPF instance 80 for each system
OSPF instances	64 (one per VRF)
OSPF interfaces	512 active, 2000 passive
OSPF LSA packet size	Jumbo packets
OSPF routes	64,000
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
RIB IPv4 routes	3 * fastpath routes
RIP instances	64 (one for each VRF)
RIP interfaces	200
RIP routes	2,500 for each VRF

	Maximum number supported
	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
Diagnostics	
Mirrored ports	479
Remote Mirroring Termination (RMT) ports	32
Filters and QoS	
Flow-based policers (IPv4 and IPv6)	16,000
Port shapers (IPv4 and IPv6)	480
Access control lists (ACL) for each chassis	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

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 16: Supported standards

Standard	Description
802.1AX	Link Aggregation Control Protocol (LACP)
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
802.1t	802.1D maintenance
802.1w-2001	Rapid Spanning Tree protocol (RSTP)
802.1X	Extended Authentication Protocol (EAP), and EAP over LAN (EAPoL)
802.1X-2004	Port Based Network Access Control
802.3 CSMA/CD Ethernet ISO/IEC 8802	International Organization for Standardization (ISO) /International Eletrotechnical Commission (IEC) 8802-3
802.3ab	Gigabit Ethernet 1000BaseT 4 pair Category 5 (Cat5) Unshieled Twisted Pair (UTP)
802.3ae	10 Gigabit Ethernet

Standard	Description
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 17: Supported request for comments

Request for comment	Description
RFC768	UDP Protocol
RFC783	Trivial File Transfer Protocol (TFTP)
RFC791	Internet Protocol (IP)
RFC792	Internet Control Message Protocol (ICMP)
RFC793	Transmission Control Protocol (TCP)
RFC826	Address Resolution Protocol (ARP)
RFC854	Telnet protocol
RFC894	A standard for the Transmission of IP Datagrams over Ethernet Networks
RFC896	Congestion control in IP/TCP internetworks
RFC903	Reverse ARP Protocol
RFC906	Bootstrap loading using TFTP
RFC950	Internet Standard Subnetting Procedure
RFC951	BootP
RFC959, RFC1350, and RFC2428	IPv6 FTP and TFTP client and server
RFC1027	Using ARP to implement transparent subnet gateways/Nortel Subnet based VLAN
RFC1058	RIPv1 Protocol
RFC1112	IGMPv1

Request for comment	Description
RFC1122	Requirements for Internet Hosts
RFC1253	OSPF
RFC1256	ICMP Router Discovery
RFC1258	IPv6 Rlogin server
RFC1305	Network Time Protocol v3 Specification, Implementation and Analysis
RFC1340	Assigned Numbers
RFC1519	Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC1541	Dynamic Host Configuration Protocol1
RFC1542	Clarifications and Extensions for the Bootstrap Protocol
RFC1583	OSPFv2
RFC1587	The OSPF NSSA Option
RFC1591	DNS Client
RFC1723	RIP v2 – Carrying Additional Information
RFC1745	BGP / OSPF Interaction
RFC1771 and RFC1772	BGP-4
RFC1812	Router requirements
RFC1866	HyperText Markup Language version 2 (HTMLv2) protocol
RFC1965	BGP-4 Confederations
RFC1966	BGP-4 Route Reflectors
RFC1981	Path MTU discovery
RFC1997	BGP-4 Community Attributes
RFC1998	An Application of the BGP Community Attribute in Multi-home Routing
RFC2068	Hypertext Transfer Protocol
RFC2131	Dynamic Host Control Protocol (DHCP)
RFC2138	RADIUS Authentication
RFC2139	RADIUS Accounting
RFC2178	OSPF MD5 cryptographic authentication / OSPFv2

Request for comment	Description
RFC2236	IGMPv2 for snooping
RFC2270	BGP-4 Dedicated AS for sites/single provide
RFC2328	OSPFv2
RFC2338	VRRP: Virtual Redundancy Router Protocol
RFC2362	PIM-SM
RFC2385	BGP-4 MD5 authentication
RFC2439	BGP-4 Route Flap Dampening
RFC2453	RIPv2 Protocol
RFC2460	IPv6 base stack
RFC2464	Transmission of IPv6 packets over Ethernet networks
RFC2545 and RFC4710	IPv6 capable BGPv4+
RFC2616	IPv6 HTTP server
RFC2710 and RFC3810	MLD (host-mode only)
RFC2740	OSPFv3
RFC2796	BGP Route Reflection – An Alternative to Full Mesh IBGP
RFC2819	RMON
RFC2918	Route Refresh Capability for BGP-4
RFC2992	Analysis of an Equal-Cost Multi-Path Algorithm
RFC3046	DHCP Option 82
RFC3065	Autonomous System Confederations for BGP
RFC3162	IPv6 RADIUS client
RFC3315	IPv6 DHCP Relay
RFC3376	Internet Group Management Protocol, v3
RFC3411 and RFC2418	SNMP over IPv6 networks
RFC3513	Internet Protocol Version 6 (IPv6) Addressing Architecture
RFC3569	An overview of Source-Specific Multicast (SSM)
RFC3587	IPv6 Global Unicast Address Format

Request for comment	Description
RFC3768 and draft-ietf-vrrp-ipv6-spec-08.txt	IPv6 capable VRRP
RFC4213	IPv6 configured tunnel
RFC4250–RFC4256	SSH server and client support
RFC4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC4861	IPv6 Neighbor discovery
RFC4862	IPv6 stateless address autoconfiguration
RFC4893	BGP support for Four-octet AS Number Space

Quality of service

Table 18: Supported request for comments

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

Network management

Table 19: Supported request for comments

Request for comment	Description
RFC1155	SMI
RFC1157	SNMP
RFC1215	Convention for defining traps for use with the SNMP
RFC1269	Definitions of Managed Objects for the Border Gateway Protocol: v3
RFC1271	Remote Network Monitoring Management Information Base

Request for comment	Description
RFC1305	Network Time Protocol v3 Specification, Implementation and Analysis3
RFC1350	The TFTP Protocol (Revision 2)
RFC1354	IP Forwarding Table MIB
RFC1389	RIP v2 MIB Extensions
RFC1757	Remote Network Monitoring Management Information Base
RFC1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1908	Coexistence between v1 & v2 of the Internet-standard Network Management Framework
RFC1930	Guidelines for creation, selection, and registration of an Autonomous System (AS)
RFC2541	Secure Shell Protocol Architecture
RFC2571	An Architecture for Describing SNMP Management Frameworks
RFC2572	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC2573	SNMP Applications
RFC2574	User-based Security Model (USM) for v3 of the Simple Network Management Protocol (SNMPv3)
RFC2575	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC2576	Coexistence between v1, v2, & v3 of the Internet standard Network Management Framework
RFC2819	Remote Network Monitoring Management Information Base

MIBs

Table 20: Supported request for comments

Request for comment	Description
RFC1156	MIB for network management of TCP/IP
RFC1212	Concise MIB definitions
RFC1213	TCP/IP Management Information Base
RFC1354	IP Forwarding Table MIB
RFC1389	RIP v2 MIB Extensions
RFC1398	Ethernet MIB
RFC1442	Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1450	Management Information Base for v2 of the Simple Network Management Protocol (SNMPv2)
RFC1573	Interface MIB
RFC1650	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC1657	BGP-4 MIB using SMIv2
RFC1724	RIPv2 MIB extensions
RFC1850	OSPF MIB
RFC2021	RMON MIB using SMIv2
RFC2096	IP Forwarding Table MIB
RFC2452	IPv6 MIB: TCP MIB
RFC2454	IPv6 MIB: UDP MIB
RFC2466	IPv6 MIB: ICMPv6 Group
RFC2578	Structure of Management Information v2 (SMIv2)
RFC2674	Bridges with Traffic MIB
RFC2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC2863	Interface Group MIB

Request for comment	Description
RFC2925	Remote Ping, Traceroute & Lookup Operations MIB
RFC2932	IPv4 Multicast Routing MIB
RFC2933	IGMP MIB
RFC2934	PIM MIB
RFC3416	v2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC4113	Management Information Base for the User Datagram Protocol (UDP)

Standard MIBs

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

Table 21: 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

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
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
STDMIB11—Evolution of the Interface Groups for MIB2	RFC2863	rfc2863.mib
STDMIB12—Definitions of Managed Objects for the Ethernet-like Interface Types	RFC1643	rfc1643.mib
STDMIB13—Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2	RFC1657	rfc1657.mib
STDMIB14—RIP version 2 MIB extensions	RFC1724	rfc1724.mib
STDMIB15—Remote Network Monitoring (RMON)	RFC2819	rfc2819.mib
STDMIB16—Open Shortest Path First (OSPF) Version 2	RFC1850	rfc1850.mib
STDMIB17—Management Information Base of the Simple Network Management Protocol version 2 (SNMPv2)	RFC1907	rfc1907.mib
STDMIB21—Interfaces Group MIB using SMIv2	RFC2233	rfc2233.mib
STDMIB26a—An Architecture for Describing	RFC2571	rfc2571.mib

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
SNMP Management Frameworks		
STDMIB26b—Message Processing and Dispatching for the SNMP	RFC2572	rfc2572.mib
STDMIB26c—SNMP Applications	RFC2573	rfc2573.mib
STDMIB26d—User-based Security Model (USM) for version 3 of the SNMP	RFC2574	rfc2574.mib
STDMIB26e—View-based Access Control Model (VACM) for the SNMP	RFC2575	rfc2575.mib
STDMIB26f —Coexistence between Version 1, Version 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

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
STDMIB38—SNMPv3 These Request For Comments (RFC) make some previously named RFCs obsolete	RFC3411, RFC3412, RFC3413, RFC3414, RFC3415	rfc2571.mib, rfc2572.mib, rfc2573.mib, rfc2574.mib, rfc2575.mib
STDMIB39—Entity Sensor Management Information Base	RFC3433	
STDMIB40—The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model	RFC3826	rfc3826.mib
STDMIB41—Management Information Base for the Transmission Control protocol (TCP)	RFC4022	rfc4022.mib
STDMIB43—Management Information Base for the User Datagram Protocol (UDP)	RFC4113	rfc4113.mib
STDMIB44—Entity MIB	RFC4133	rfc4133.mib
STDMIB46—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 22: 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

Proprietary MIB name	File name
PROMIB5 - Other SynOptics definitions	s5emt103.mib
PROMIB6 - Avaya RSTP/MSTP proprietary MIBs	nnrst000.mib, nnmst000.mib
PROMIB7 - Avaya IGMP MIB	rfc_igmp.mib
PROMIB8 - MIAvayal IP Multicast MIB	ipmroute_rcc.mib
PROMIB9 - Avaya PIM MIB	pim-rcc.mib
PROMIB11 - Avaya MIB definitions	wf_com.mib

Chapter 6: Upgrading

This chapter provides important information about upgrading the system software. For more details about upgrades and patches, see *Avaya Virtual Services Platform 9000 Upgrades and Patches* , NN46250–400.

Upgrading IST peer switches from Release 3.0.x

Review the entire upgrade procedure to ensure that you clearly understand all of the steps and collect any required information about port assignments before you proceed with the upgrade. If you are unclear on any of the procedure steps, contact Avaya Technical Support before you proceed with the upgrade.

Before you begin

- You have transferred the Release 3.2.0.0 files to both nodes.
- Ensure that you have access to both systems. Avaya recommends that you perform this upgrade by using a console cable. If you do not have console-cable access, and your session flows over a non-SMLT connected port, ensure that you do not shut down the port that you use to perform the upgrade procedure.

About this task

When you upgrade a pair of core switches that connect through an IST peer connection, you must take special care. Issue wi00859221 forced a change in the processing of the IST control channel on the system. This change prevents the IST protocol from establishing a connection between a switch that runs Release 3.0.0.0 and a switch that runs Release 3.0.1.x, 3.1.0.0, or later.

Perform this procedure to upgrade the two peer switches and minimize the network downtime. The following figure shows two switches that use an IST peer connection. In the example, the following ports are the SMLT ports:

- SMLT 1 uses ports 4/2, 4/14, 4/26, 4/38.
- SMLT 4 uses ports 4/13, 4/25, 4/37.
- SMLT 500 uses port 4/47.

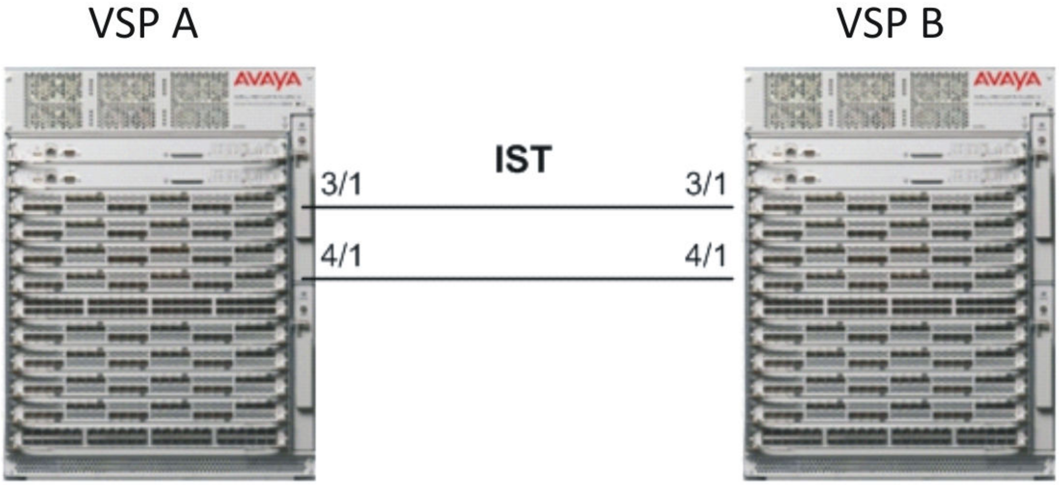

Figure 1: IST peer configuration

Procedure

1. Log on to the console ports for each device.
2. Save the running configuration to ensure that it is correctly retrieved after you reset the systems:

   ```
   save config
   ```
3. Add the software release on both nodes of the cluster:

   ```
   software add VSP9K.3.2.0.0.tgz
   software add-modules 3.2.0.0 VSP9K.3.2.0.0_modules.tgz
   ```
4. Activate the software release on both nodes of the cluster:

   ```
   software activate VSP9K.3.2.0.0
   ```
5. On the first device, shut down all SMLT ports, leaving the IST ports up.

   ```
   enable
   config t
   int gig 4/2,4/14,4/26,4/38,4/13,4/25,4/37,4/47
   shutdown
   ```

   Note:

   For simplicity, you can shut down all non-IST ports on the system, however, this will cause systems that connect by using non-SMLT ports to experience a longer outage as you complete the upgrade procedure. You can obtain a list of SMLT ports by using the `show mlt` command, and noting the port members from all MLTs where the `MLT ADMIN` column shows `smlt`.

6. Verify that SMLT traffic has switched over to the SMLT cluster peer node.
7. Reset the first device:

   ```
   reset —y
   ```

   The device resets and starts in approximately 3–4 minutes.
8. After the device starts, log on with read and write privileges to commit the software:

   ```
   enable

   software commit
   ```

   The first VSP 9000 now runs the new software version. The SMLT ports on the first node will be locked and physically link down while the IST channel attempts to establish a connection to the peer node. The IST will not be established because of the mismatched IST control channel. After approximately 60 seconds, the SMLT ports on the first node will automatically unlock and come back up.

   Important:

   You must wait for the ports to unlock and come back up before you proceed to the next step of this procedure. Failure to wait will result in traffic loss.

   Perform the remaining procedure steps on the second device.
9. On the second device, shut down all SMLT ports, leaving the IST ports up.

   Note:

   In this example, the SMLT port assignments are the same on VSP A and VSP B. The port numbers may differ between the peer nodes in your configuration.

   ```
   enable

   config t

   int gig 4/2,4/14,4/26,4/38,4/13,4/25,4/37,4/47

   shutdown
   ```

   Note:

   For simplicity, you can shut down all non-IST ports on the system, however, this will cause systems that connect by using non-SMLT ports to experience a longer outage as you complete the upgrade procedure. You can obtain a list of SMLT ports by using the `show mlt` command, and noting the port members from all MLTs where the `MLT ADMIN` column shows `smlt`.
10. Verify that SMLT traffic has switched over to the SMLT cluster peer node.
11. Reset the second device:

    ```
    reset —y
    ```

    The device resets and starts in approximately 3–4 minutes.

12. After the device starts, log on with read and write privileges to commit the software:

    ```
    enable
    ```

    ```
    software commit
    ```

    After the restart, both devices use the same version of software and IST channel. The IST channel is reestablished and SMLTs return to a working state.

13. Verify the IST state for the IST channel is up:

    ```
    show ist mlt
    ```

    ```
    =====================================================================
                                      Mlt IST Info
    =====================================================================
    MLT   PEER-IP                VLAN     ENABLE   IST
    ID    ADDRESS                ID       IST      STATUS
    ---------------------------------------------------------------------
    2    10.254.172.2            172      true     up


    NEGOTIATED                                      MASTER/
    DIALECT      IST STATE                          SLAVE
    ---------------------------------------------------------------------
    v1.0         Up                                 Slave
    ```

14. Verify the current state of the IST and active SMLTs. The following example shows only partial command output.

    ```
    show mlt
    ```

    ```
    =====================================================================
                                        Mlt Info
    =====================================================================
                            PORT     MLT    MLT         PORT         VLAN
    MLTID IFINDEX NAME      TYPE    ADMIN CURRENT    MEMBERS        IDS
    ---------------------------------------------------------------------
    1   6144  SMLT-1       trunk   smlt   smlt     4/2,4/14,4/26,4/38
    2 3 4
    2   6145  IST-MLT      trunk   ist    ist      3/1, 4/1
    2 3 4 172 200 500
    4   6147  SMLT-4       trunk   smlt   smlt     4/13,4/25,4/37  4
    100 6243  MLT-100      trunk   norm   norm     4/23-4/24,4/27-4/28
    100
    500 6643  SMLT-500     trunk   smlt   norm     4/47              500

    All 5 out of 5 Total Num of mlt displayed
    ```

Chapter 7: 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 23: Known issues

Issue number	Description	Workaround
wi00519967	Log filtering based on date and time is currently unavailable.	—
wi00768362	The **`show alarm database`** command does not show the CPU from which the alarm originated. The log report contains this information.	Use the **`show logging file alarm`** command to check the complete details and the CPU from which the alarm originated.
wi00828941	After an HA failover, if KHI polling polls the other CP, but that CP is still starting, the KHI poll times out and a letter sync error message appears.	For the next KHI poll the CP will be up and will respond. This error message is not service impacting and can be ignored.
wi00969817	When you configure an access policy for SSH access, and an SSH session is attempted and blocked due to the access policy, there is no message logged in the VSP 9000 system log to	—

Issue number	Description	Workaround
	indicate that a session was blocked.	
wi00974862	The **sys ecn-compatibility** command to enable explicit congestion notification does not apply to VSP 9000.	—
wi00975675	When you disable and then enable VSP Talk, no log message indicates that VSP Talk is enabled.	—
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.

Applications

Table 24: Known issues

Issue number	Description	Workaround
wi00940744	The command **show application vsptalk client** does not show connection status.	View this information in the log file.
wi00975662	When you use the **vsptalk gtalk enable** command, the system checks for an IPv4 DNS configuration. If a DNS primary name server is not configured, VSP Talk does not connect to the Google Talk IM server.	Configure an IPv4 DNS primary DNS server first and then second and tertiary name servers. If you remove a primary DNS name server, move the secondary (or tertiary) name server to become the primary name server.

Chassis operations

Table 25: Known issues

Issue number	Description	Workaround
wi00564595	If there is not enough power available in the chassis to power all cards when the system is powered up, one or more cards will not be powered on. Configuration for these cards will be ignored. When enough power is available the cards will be automatically powered up but they will not automatically receive their configuration.	To download the configuration to any cards that experience delayed boot up, source the configuration for that card.
wi00891718	Unable to access `/usb` from the peer CP.	Use TFTP from the peer or configure the network management port and use a transport protocol like FTP or TFTP, directly to the secondary CP.
wi00930215	After you use the **`extflash-stop`** command to unmount the external Compact Flash, you must remove and reinsert the Compact Flash to remount the volume.	—
wi00967400	You can see the following message at system start: `GlobalRouter HW ERROR portGetPortNum: invalid physical port 0724`. This message has no functional impact and can be ignored.	—
wi00968592	A KHI warning message can appear after you stop and remove a USB device. This message is not functionally	—

Issue number	Description	Workaround
	impacting and can be ignored.	
wi00969922	If you remove the backup CP module, you can see the following output on the console: `fbuf allocated in "/vob/cb/nd_platform/chassis/lib/ch_sync.c" at line 341 is freed` This message occurs if an application tries to synchronize data to the backup CP module at the same time that you remove the module.	This message has no functional impact and can be ignored.
wi00970236	The default value for the loadingconfig time is 15 minutes. The configurable range for the **`boot config loadconfigtime`** command is 0 to 300 seconds. If you configure a value that is less than the default, the device still uses the default value to validate the loading time. Because the maximum configurable value is 300 seconds, the value is always less than the default and does not take effect. The intent of the parameter is the time to load the configuration. The timer that runs in the VSP 9000 actually tracks the full start time, for example, the time spent waiting for other IO ready and to download port MAC.	—
wi00988403	If you configure the IPFIX collector parameters, the configuration does not save correctly. After you save the	Do not use IPFIX in this release. This issue will be resolved in a future software release.

Issue number	Description	Workaround
	configuration, if the verify_config flag is TRUE, the configuration will not boot. If the verify_config flag is not TRUE, the parameter is skipped on boot.	

COM

Table 26: Known issues

Issue number	Description	Workaround
wi00949006	You cannot view more than 50 ARP entries using COM.	In ACLI, use **`show ip arp`**. In EDM, use **Configuration** > **IP** > **IP** > **ARP**.

EDM

Table 27: Known issues

Issue number	Description	Workaround
wi00668629	After deleting a VRF, all open EDM sessions that are using that VRF need to be closed manually by the user.	—
wi00825617	EDM may display port 1/48 in the VLAN forwarding table.	This port is shown in error and can be ignored.
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.	—

Issue number	Description	Workaround
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.
wi00962229	EDM does not show the TTL field in the ARP table.	Use ACLI.
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.
wi00968931	You cannot configure EDM to use an IPv6 address for the Help directory on a TFTP server.	Use an IPv4 TFTP server. Store the Help files on the IPv4 TFTP server, and then configure EDM to use the IPv4 server address.
wi00975479	The VLAN range for a brouter port should be 2 to 4084.	—
wi00975511	You cannot delete a static IGMP group using EDM.	Use ACLI.
wi00978158	You can configure IPv6**ReversePathCheckEnable** and **ReversePathCheckMode** on an IPv6 management interface even though this configuration has no meaning. The message `undoFailed` appears on EDM, and SW errors appear on the CP console. You can ignore these errors.	—
wi00984551	You cannot configure an IPv6 tunnel using EDM.	Use ACLI.

HA operations

Table 28: Known issues

Issue number	Description	Workaround
wi00937861	The **`exception dump max-disk-space`** configuration ACLI command is not available on the standby CPU.	—

Management and general administration

Table 29: 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.
wi00932777	The current release does not support IPv6 addresses for the **`traceroute`** command. VSP 9000 will add IPv6 traceroute support in a future release.	—
wi00972377	Do not use spaces in an SNMP group. If you do use space, two errors print several times.	To use the default, enter an empty string as two quotation marks without a space, for example, "". Do not use quotation marks with a space between them, for example, " ", The last entry generates errors.

Issue number	Description	Workaround
wi00974849	You cannot disable the UDP checksum.	—
wi00977397	You may be unable to use the `ls` command if you create an FTP connection over IPv6 from a Windows client. The display freezes for 30 seconds and the list does not display.	Use the `dir` command.
wi00980950	If the link from the VRRP master back to the edge goes down, the ICMP ping from the edge to the VRRP virtual interface fails in the following scenario: • A triangle SMLT configuration with VRRP, where ICMP ping to the virtual IP interface from the edge hashes to two different paths: a. Traffic to the core to the VRRP backup master. b. The return path from the VRRP master back to the edge. There is no impact to other data packets. After the link is restored, ICMP ping to the VRRP virtual interface will work as expected.	—

wi00981422	Some ACLI commands allow you to configure and enable the feature in a single command. However, some of these command result in an error because certain entries must be created before they can be enabled.
	For example, the **`ipv6 dhcp-relay fwd-path 9:1:1::2 1::2 enable`** command results in the following error: `Error:`
		Create the entry, and then enable the entry by using two separate commands. For example:
		`ipv6 dhcp-relay fwd-path 9:1:1::2 2::1`
		`ipv6 dhcp-relay fwd-path 9:1:1::2 2::1 enable`

Issue number	Description	Workaround
	`rcIpv6DhcpForwardTblSet failed for IfIndex 2050. Make sure the path is created before you enable it.`	

MLT, SMLT, and link aggregation

Table 30: 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.
wi00976726	The **`show lacp int mlt x`** command will show information for nonexistent MLTs (information is correct), rather than not showing any information at all.	—
wi00976736	The maximum range for the IfIndex in the **`show lacp interface`** command is 6399 when it is actually 6655.	—

Multicast

Table 31: Known issues

Issue number	Description	Workaround
–	The ACLI query-interval parameter for PIM interfaces and ports is changed to hello-	—

Issue number	Description	Workaround
	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.	
–	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: 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.	—

Patching

Table 32: Known issues

Issue number	Description	Workaround
wi00511642	The **`software patch commit`** and **`software patch remove`** commands will not display messages such as Syncing release directory on backup CP card in slot 2 while executing the command in a Telnet session.	—
wi00732444	After a patch is reverted the patch action should be committed before moving on	The remove command will not take effect until the commit is explicitly or

Issue number	Description	Workaround
	with more actions. The commit may be explicitly typed or the commit can occur via auto-commit after the configured timeout period. In this case the remove command was allowed and operated correctly without an error or warning indicating that it would not take effect until the commit occurred explicitly or via timeout.	automatically executed after a patch is reverted.
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.
wi00966662	If you issue a hitless patching revert command against an active applied hitless patch, there may be a short processing delay that can affect VLACP.	To avoid link flapping during a patch revert, verify VLACP is configured to the recommended minimum value of 500ms and 5 retries during the revert.
wi00971012	If you reset the chassis prior to committing a patch, the system clears the patch. A reset patch does not require an **`abort`** command. You do not need to enter an **`abort`** command after a reset even for a hitless patch. The reset clears the patch. If you do use an **`abort`** command after the reset, you will see a message that instructs you to reset the shelf to rollback the patch. The chassis has already	—

Issue number	Description	Workaround
	rolled-back and no further reset is required.	

QoS and filters

Table 33: Known issues

Issue number	Description	Workaround
wi00970134	If you use egress filters with multicast traffic, using the VLAN attribute in the ACE to match the outgoing VLAN does not work.	Use any other attribute to filter the packets.
wi00970587	If a configuration file with filter configuration is sourced on a switch that already has filters configured, FILTER and HW errors can occur. This does not cause any functional impact and can be ignored.	—

Routing

Table 34: Known issues

Issue number	Description	Workaround
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	—

Issue number	Description	Workaround
	system is not effected because the master CP stays operational.	
wi00962267	IPv6 Duplicate Address Detection (DAD) does not work on 10 Gb interface modules. If you configure duplicate IPv6 addresses between the VSP and another node on a 10 Gb link, the VSP software does not detect the duplicate scenario.	—
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.	—

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 35: 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.		
wi00565499	If you use VSP and Ethernet Routing Switch 8600 on a VLAN, and all	Disable the links on the Ethernet Routing Switch	

Issue number	Description	Workaround	Fixed in release
	systems operate in MSTP mode, a loop can be generated if you restart a VLAN port on the Ethernet Routing Switch.	8600 to remove the loop.	
wi00689238	If a VSP 9000 aggregation switch sends a high volume (more than 3000) of OSPF or RIP routes to an Ethernet Routing Switch 8600 edge device to redistribute into an OSPF domain, the CPU utilization of the edge device can increase, which results in dropping all VLACP packets from the VSP device. The VLACP link operational state is down.		ERS 5.1.6.0
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

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 36: 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.

Issue number	Description	Workaround
wi00854206	For VLACP enabled links, recommended values exist for the configuration of the VLACP timers. However, in an SMLT topology, with VLACP and multicast both enabled on the SMLT link, you may need to adjust or increase the VLACP timers on that link to accommodate for a scaled multicast environment where there is a higher processing load on the CP, especially during failover events. This higher load can affect the ability to process VLACP keep-alive messages in a timely manner, which can cause the link to flap. You may need to configure timers proportionately to the anticipated multicast route load.	Avaya recommends that you configure IST links with a VLACP timeout of long, timeout scale of 3, and slow-periodic-time of 30 000 ms. These links are not impacted by multicast scaling considerations.

Chapter 8: Resolved issues

This section identifies the issues resolved in this release.

Alarm, logging, and error reporting

Table 37: Resolved issues

Issue number	Issue description
wi00731983	If the external compact flash card is removed from the chassis after it boots, and the alarm log has not been redirected to use internal flash before removing the external flash, the alarm write file will fail with errors printed on the console.
wi00828938	Some messages currently tagged as errors should be tagged as warnings. Read the body of the message to determine the severity of the situation the message is reporting.
wi00832713	VLACP can display an incorrect timestamp on the port up time.
wi00857881	Ability to send CLI or SNMP logs to a syslog server. For more information, see New features on page 11.
wi00866334	Logger task can be overrun by excessive log messages, which causes a CP module to stop responding.
wi00972477	OSPF ERROR level messages may be displayed on the console when an IO slot is removed and reinserted. These messages do not indicate a problem, and now appear only in the log file.

Chassis operations

Table 38: Resolved issues

Issue number	Issue description
wi00820546, wi00822103	The VSP 9000 does not support hot insert of multiple modules simultaneously in this release.
wi00868954	Ability to hot swap external Compact Flash from a CP module. For more information, see Removing external storage devices from the CP module on page 19.
wi00892575	The default value of CP limit for a port is 8000 packets per second (configurable range is 1,000–20,000). This value is the number of packets received by the CPU on the CP module that ingressed the VSP on a particular IO port. In Release 3.1, this number is not accurate on port 3/1 because IPFIX and MAC Learning packets are taken into account.
wi00892803	Repeated runs of the **`show sys-info card`** command can result in a crash.
wi00968475	USB device was not recognized after upgrade of compact flash on Release 3.1.
wi00971030/wi00968460	Issuing a **`show`** command while the system is in the process of a CPU switchover can result in a core.

COM

Table 39: Resolved issues

Issue number	Issue description
wi00949750	EDM COM plugin does not display all IP routes.

Issue number	Issue description
wi00958878	A user can disable or enable ports using COM or EDM on devices despite the fact that the devices are not assigned to the user.

EDM

Table 40: Resolved issues

Issue number	Issue description
wi00520403	The EDM Idle timer is set to 15 minutes. If an HTTP request is received after the idle timer has elapsed, the web server returns the message response `Not Authorized`.
wi00685977	EDM queries data in the background which may be used on a screen. If this data retrieval encounters an issue, a message will be displayed related to the failure. This error message may not directly relate to the context of what the user is currently viewing.
wi00831460	In EDM, no filter option is available on ARP and Route tabs to sort through many pages of data.
wi00845679	You cannot modify, delete, or add the management IP address on the standby CP using EDM.
wi00869366	EDM does not sort the **Configuration** > **IP** > **IP** > **ARP Interface**column by using the field text.
wi00884199	You cannot open EDM Help files if you access the system over an HTTPS connection using Internet Explorer.
wi00900509	The OSPF protocol tab is missing from the IP section of all VLANs within the Global Router context, which results in the inability to configure OSPF or modify the OSPF configuration on a VLAN that is part of the Global Router context.

Issue number	Issue description
wi00941147	If you use EDM to create an access policy, you cannot configure the ID number as you can through ACLI.
wi00958878	A user can disable or enable ports using COM or EDM on devices despite the fact that the devices are not assigned to the user.
wi00968568	EDM does not display the **LastRunTimeConfigSave** value correctly.
wi00968805	You cannot configure spoof-detect through EDM.
wi00971070	A crash may occur while deleting an ARP entry though EDM

Management and general administration

Table 41: Resolved issues

Issue number	Issue description
wi00896935	FTP connections fail when the expected user authentication method is a configured RADIUS server.
wi00971250	Abnormally terminating Telnet or SSH sessions can result in loss of connectivity to the CP module.

MLT, SMLT, and link aggregation

Table 42: Resolved issues

Issue number	Issue description
wi00510386	When all members of a MLT go down there is no trap generated.
wi00885466	This issue occurs if you have a network with two VSP devices, VSP-A and VSP-B, in the

Issue number	Issue description
	core, that connect to an edge device, EDGE-C, which runs SMLT to VSP-A and VSP-B. If you move a device that connects to Edge-C to connect it directly to a port on one of the VSP devices, you must reboot the device after you connect it to the VSP port. The reboot initiates traffic, which reestablishes the MAC and ARP tables. If the device does not initiate traffic, it may not be reachable by other devices until it initiates traffic.
wi00890291	If you remove a port from SMLT, you cannot disable spanning tree on that port until the port is up.
wi00890294	If you add a port with a copper interface to an MLT group, each port in the MLT bounces in sequence. For example, if ports 1 and 2 are in an existing MLT and you add port 3, port 1 bounces, and then port 2 bounces. The MLT does not drop because at least one port is always up.
wi00894948	If you configure port 48 of a 9048GT or 9048GR module in ERS slot 12 as an SMLT port, after you reset the VSP 9000, the SMLT port will not come up.
wi00962378	The **`show running-config`** command displays `loop-detect action mac-discard` although it cannot be configured on an IST port.

Patching

Table 43: Resolved issues

Issue number	Issue description
wi00862528	If you revert a patch, all ACLI sessions terminate except the one you used to issue the **`software patch revert`** command. The system reverts the patch correctly but you must reestablish all other ACLI sessions.

QoS and filters

Table 44: Resolved issues

Issue number	Issue description
wi00967392	If you configure the filter option copy-to-pcap, the VLAN tag priority of ingressing packets is changed in the captured copy.

Routing

Table 45: Resolved issues

Issue number	Issue description
wi00732579	Due to MAC management limitations for IPv6 in this release, Avaya does not recommend configuring both IPv4 and IPv6 on one specific interface simultaneously.
wi00886060	The ACLI command **`show ip vrrp interface`** does not show VRRP details for brouter ports.
wi00893208	The **`show ip rip interface`** command displays configured Circuitless IP (CLIP) interfaces, even though RIP is not enabled on these interfaces. This issue is a display issue with this command.
wi00893529	If you configure more than one inter-VRF redistribution policy from and to the same source or destination VRF, disabling one policy disables both policies. For example, if you configure redistribution policies for both OSPF and RIP from GRT to VRF1, disabling the OSPF policy also disables the RIP policy.
wi00893530	If you delete an inter-VRF redistribution policy after an HA failover, the redistributed routes may not be removed from the forwarding table.

Issue number	Issue description
wi00897422	DHCP Option 82 has an artificial limit of 64 bytes for the options field. After this limit is exceeded, the VSP 9000 does not add the option 82 information to the packet. This limit prevents DHCP Option 82 from working in Windows environments.

VLAN operations

Table 46: Resolved issues

Issue number	Issue description
wi00850312	If you delete the IPv6 address and IPv4 address from a VLAN interface, adding the IPv4 address again fails.
wi00908730	When an ARP request is generated from an NLB server, the request uses VRF 0 instead of a proper VRF.

Chapter 9: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.