Release Notes — Release 3.1
Avaya Virtual Services Platform 9000

3.1
NN46250-401, 02.04
July 2011

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 Web sites 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 Web site: 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.

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”).

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 Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: New in this release

The following sections detail what's new in *Avaya Virtual Services Platform 9000 Release Notes* (NN46250–401) for Release 3.1:

- Features on page 5
- Other changes on page 6

Features

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

Feature licensing

Feature licensing on page 20 is added to clarify how the 60–day trial license operates and what you need to do after it expires.

Hardware support

Release 3.1 changes the minimum requirement for Switch Fabric (SF) modules in the chassis. For more information, see New features on page 9

New features

Release 3.1 provides or enhances support for the following features:

- backup and restore compact flash
- DHCP Relay Option 82
- IPFIX for IPv4
- update to Key Health Indicators
- Layer 3 remote mirroring
- Microsoft NLB ARP multicast-MAC-flooding support
- multicast statistics
- Secure Shell client

For more information, see the following sections:

- New features on page 9
- Supported RFCs on page 30
- Software scaling capabilities on page 24

Upgrading IST peer devices from Release 3.0.0.0

You must perform a specific upgrade procedure if you use two Virtual Services Platform 9000 Release 3.0.0.0 devices in the core in an IST peer relationship. For more information, see Upgrading IST peer switches on page 41.

Other changes

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

Fixes from previous releases

Fixes from previous releases on page 20 is added to the document.

Resolved issues

Resolved issues on page 57 is added to the document.

Known issues

Known issues on page 45 is updated.

Interoperability issues on page 53 is added to the document to identify issues specific to the interoperability of this product with other Avaya products.

Limitations on page 55 is added to the document to identify known limitations or expected behaviors that may first appear as if they are issues.

Chapter 2: Introduction

This document describes the features and known issues of the Avaya Virtual Services Platform 9000 Release 3.1. Use this document to help you optimize the functionality of your device.

- Important notices and new features on page 9
- Software and hardware scaling capabilities on page 23
- Supported standards, request for comments, and Management Information Bases on page 29
- Upgrading on page 41
- Known issues and limitations on page 45
- Resolved issues on page 57

Avaya Virtual Enterprise Network Architecture (VENA) expands proven Avaya data center solutions and leverages existing data network infrastructures and investments. In the coming months the Virtual Services Platform 9000 will be enhanced to become a major component of Avaya VENA solutions.

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 on page 9
- Supported hardware on page 10
- File names for this release on page 16
- Important information and restrictions on page 16

New features

The following sections highlight the feature support added in Release 3.1.

Backup and restore compact flash

Release 3.1 adds the ability to backup and restore the contents of compact flash to a USB flash device. For more information see *Avaya Virtual Services Platform 9000 Administration* (NN46250–600) and *Avaya Virtual Services Platform 9000 Commands Reference — ACLI* (NN46250–104).

DHCP Relay Option 82

Release 3.1 supports DHCP Relay Option 82. The relay agent inserts this option when it forwards client-originated DHCP packets to a DHCP server. For configuration information, see *Avaya Virtual Services Platform 9000 Configuration — IP Routing Protocols* (NN46250–505). For statistics information, see *Avaya Virtual Services Platform 9000 Performance Management* (NN46250–701). Note that no command exists to clear DHCP Relay statistics. To reset the statistics counters to zero, you must use the **`sys action reset counters`** command.

IPFIX for IPv4

Release 3.1 adds hardware-based IPFIX capabilities. Internet Protocol Flow Information eXport (IPFIX) is an Internet Engineering Task Force (IETF) standard that monitors and exports IP flow information.

For more information about IPFIX, see *Avaya Virtual Services Platform 9000 Performance Management* (NN46250–701).

Update to Key Health Indicators

Release 3.1 adds new show and clear commands for Key Health Indicators (KHI) statistics. For more information, see *Avaya Virtual Services Platform 9000 Fault Management* (NN46250–703).

Layer 3 remote mirroring

Release 3.1 supports Layer 3 remote mirroring for ports and flows. Layer 3 remote mirroring monitors traffic from multiple network devices across an IP network, and sends that traffic in an encapsulated form to the destination analyzers. For more information, see *Avaya Virtual Services Platform 9000 Troubleshooting* (NN46250–700).

Microsoft NLB ARP multicast-MAC-flooding support

Release 3.1 extends multicast MAC flooding for Network Load Balancer (NLB). Use the ARP MAC-flooding option to support multiple NLB clusters in the same VLAN. For more information, see *Avaya Virtual Services Platform 9000 Configuration — VLANs and Spanning Tree* (NN46250–500).

Multicast statistics

Release 3.1 supports multicast route statistics associated with group IP addresses. For more information, see *Avaya Virtual Services Platform 9000 Performance Management* (NN46250–701).

SSH client support

Beginning with Release 3.1, you can use the Secure Shell (SSH) protocol for both inbound and outbound access with the Virtual Services Platform 9000. For more information, see *Avaya Virtual Services Platform 9000 Administration* (NN46250–600).

Switch Fabric support

Beginning with Release 3.1, you must install a minimum of three SF modules in the chassis. Install an SF module in slots SF1 and SF4; install a third SF module in one of the remaining slots. Releases prior to 3.1 required a minimum of four SF modules.

Supported hardware

This section details the hardware components of the Avaya Virtual Services Platform 9000.

New hardware

No new hardware is added for Release 3.1.

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 Control Processor (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 architecture provides redundancy while two CP modules are used in a system. The 9080CP module measures 23 inches in length.

The Virtual Services Platform 9000 9080CP module supports the following interfaces:

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

The Compact Flash card is mandatory. You must install this card in the CP module before you provide power to the module. The Compact Flash card is not hot swappable. You can order the following external storage devices 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

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

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.

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 Virtual Services Platform 9000.

Table 4: Supported SFP and SFP+ fiber connectors

Model number	Product number	Description
10GBASE-SR/SW	AA1403015-E6	850 nanometers (nm). The range is up to • 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.

Model number	Product number	Description
10GBASE-CX	AA1403018-E6 to AA1403021-E6	4-pair twinaxial copper cable to connect 10 Gb ports. The maximum range is 15 m.
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	Up to 10 km reach over a single mode fiber (SMF) pair. Up to 550 m reach over a multimode fiber (MMF) pair.
1000BASE-XD	AA1419050-E6	1310 nm, up to 40 km over SMF pair.
	AA1419051-E6	1550 nm (non-CWDM), up to 40 km over SMF pair.
1000BASE-ZX	AA1419052-E6	1550 nm (non-CWDM), up to 70 km over SMF pair.
1000BASE CWDM	AA1419053-E6 to AA1419060-E6	1470 nm to 1610 nm (CWDM) 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 Virtual Services Platform 9000

Table 5: Supported SFP connectors

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	1310nm up to 10km
	AA1419076-E6	1310nm up to 40km
1000BASE-BX-D	AA1419070-E6	1490nm up to 10km
	AA1419077-E6	1490nm 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	1310nm, 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.

File names for this release

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

Software files

The following table gives the details of the Virtual Services Platform 9000 Release 3.1 software files.

Table 6: Software files

File name	Description	Size
VSP9K.3.1.0.0.tgz	Release 3.1 archived distribution	93 MB
VSP9K.3.1.0.0_modules.tgz	Encryption modules	33 KB

Open Source software files

The following table gives the details of the Open Source software files distributed with the Virtual Services Platform 9000 Release 3.1 software.

Table 7: Open Source software files

File name	Description	Size
VSP9K.3.1.0.0_Copyright.mht	Master copyright file. This file is located in the Licenses directory.	351 KB
VSP9K.3.1.0.0_OpenSource.zip	Open source base software for Virtual Services Platform 9000 Release 3.1.	310 MB

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

Important information and restrictions

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

Protecting modules

⚠ **Caution:**

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

Note:

You must install the external Flash card media for your CP module prior to power on of the chassis and CP modules.

⚠ **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.

Supported browsers

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

- Microsoft Internet Explorer 7.0
- Mozilla Firefox 3.0 and above

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	0C	40C
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	-25C	70C
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

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.

IPv6 addressing

Avaya supports IPv6 addressing with Ping, Telnet, and SNMP access to the switch. It does not currently support SSH, FTP, TFTP, RLOGIN, SCP or other access methods.

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.

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 3.1 incorporates all fixes from prior releases, up to and including, Release 3.0.2.0.

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

Chassis, switching fabrics, and control processors			Minimum software version	Part number
Power Supplies				
	9006AC	1200–2000W AC Power Supply	3.0	EC1405001-E6
Cooling modules				
	9012SC	Side Fan Tray	3.0	EC1411001-E6
	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)

Chassis, switching fabrics, and control processors			Minimum software version	Part number
	1000BASE-EX DDI SFP	1550 nm, Gigabit Ethernet, duplex LC connector	3.0	AA1419071-E6
	1000BASE DDI CWDM 40 km SFP	Gigabit Ethernet, duplex LC connector	3.0	AA1419053-E6 to AA1419060-E6.
	1000BASE DDI CWDM 70 km SFP	Gigabit Ethernet, duplex LC connector	3.0	AA1419061-E6 to 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 the Avaya Virtual Services Platform 9000.

- Hardware scaling capabilities on page 23
- Software scaling capabilities on page 24

Hardware scaling capabilities

This section lists hardware scaling capabilities of the 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
9012 Chassis	
Control Processor (CP) modules	2
Console port	1 D-subminiature 25-pin shell 9 pin connector (DB9)
Ethernet management	1 Registered Jack (RJ) 45

	Maximum number supported
USB port	1 Universal Serial Bus (USB) Type A (Master)
Compact flash	1
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

Software scaling capabilities

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

Table 15: Software scaling capabilities

	Maximum number supported
Layer 2	
IEEE/Port-based VLANs	4,084
Protocol-based VLANs	16
Internet Protocol (IP) Subnet-based VLANs	256
Source MAC-based VLANs	100
Multiple Spanning Tree Protocol (MSTP)	64 instances
Rapid Spanning Tree Protocol (RSTP)	1 instance
MACs in forwarding database (FDB)	128K
Multi-Link Trunking (MLT)	512 groups
Split Multi-Link Trunking (SMLT)	511 groups
Inter-Switch Trunk (IST)	1 group
S/MLT Ports per group	16
LACP	512 aggregators

	Maximum number supported
LACP ports per aggregator	8 active and 8 standby
VLACP Interfaces	128
SLPP	500 VLANs
Layer 3	
Internet Protocol version 4 (IPv4) Interfaces	4,343
IP interfaces (Brouter)	480
Circuitless IP interfaces	256
ARP for each port, VRF, or VLAN	64,000 entries total
Static Address Resolution Protocol (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
FIB IPv4 routes	500,000
RIB IPv4 routes	3 * fastpath routes
ECMP routes	64,000
ECMP routes (fastpath)	8
Routing policies (IPv4)	512
IPv4 VRF instances	512
RIP instances	64 (one for each VRF)
RIP interfaces	200
RIP routes	2,500 for each VRF 10,000 for each system
OSPF instances	64 (one per VRF)
OSPF interfaces	512 active, 2000 passive
Open Shortest Path First (OSPF) adjacencies	512
OSPF areas	12 for each OSPF instance 80 for each system
OSPF LSA packet size	Jumbo packets
OSPF routes	64,000
BGP peers	256
BGP Internet peers (full)	3
BGP routes	1.5 million
IP Routing policies (IPv4)	500 for each VRF

	Maximum number supported
	5,000 for each system
IP Prefix List	500
IP Prefix entries	25 000
RSMLT interfaces	4,000 over 128 SMLT interfaces
Multicast IGMP interfaces	4,084
Multicast source and group (S, G)	6,000
PIM interfaces	512 active; 4084 passive
VRRP interfaces	255 for each VRF 512 for each system
VRRP interfaces fast timers (200ms)	24
UDP/DHCP Forwarding entries	512 for each VRF 1,024 for each system
NLB Clusters — Unicast	128 for each VLAN 2,000 for each system
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
IPv4 Telnet sessions	8
IPv6 Telnet sessions	8
IPv4 FTP sessions	4
IPv4 Rlogin sessions	8
Filters and QoS	
Flow—based policers	16,000
Port shapers	480
Access control lists (ACL) for each chassis	2,048
Access control entries (ACE) for each chassis	16,000
ACEs per ACL (a combination of Security and QoS ACEs)	1,000
Unique redirect next hop values for ACE Actions	2,000
Diagnostics	
Mirrored ports	479
Remote Mirroring Termination (RMT) ports	32

	Maximum number supported
Operations, Administration, and Maintenance	
IPFIX flows	96,000 for each interface module 960,000 for each chassis

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 the Avaya Virtual Services Platform 9000 supports.

Supported standards

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

Table 16: Supported standards

Standard	Description
802.3 CSMA/CD Ethernet ISO/IEC 8802	International Organization for Standardization (ISO) /International Eletrotechnical Commission (IEC) 8802-3
802.3i	10BaseT
802.3u	100BaseT
802.3z	Gigabit Ethernet
802.3ab	Gigabit Ethernet 1000BaseT 4 pair Category 5 (Cat5) Unshieled Twisted Pair (UTP)
802.1AX	Link Aggregation Control Protocol (LACP)
802.3ae	10 Gigabit Ethernet
802.3an	10 Gigabit Copper
802.1Q	Virtual Local Area Network (VLAN) tagging
802.3x	flow control

Standard	Description
802.1p	VLAN prioritization
802.1t	802.1D maintenance
802.1w-2001	Rapid Spanning Tree protocol (RSTP)
802.1s	Multiple Spanning Tree Protocol
802.1X	Extended Authentication Protocol (EAP), and EAP over LAN (EAPoL)
802.1X-2004	Port Based Network Access Control

Supported RFCs

The following table and sections list the RFCs that the 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 Sub-Netting Procedure
RFC951	BootP
RFC1027	Using ARP to implement transparent subnet gateways/Nortel Subnet based VLAN
RFC1058	RIPv1 Protocol

Request for comment	Description
RFC1112	IGMPv1
RFC1122	Requirements for Internet Hosts
RFC1253	OSPF
RFC1256	ICMP Router Discovery
RFC1305	Network Time Protocol v3 Specification, Implementation and Analysis3
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
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
RFC2236	IGMPv2 for snooping

Request for comment	Description
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
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
RFC3376	Internet Group Management Protocol, v3
RFC3513	Internet Protocol Version 6 (IPv6) Addressing Architecture
RFC3569	An overview of Source-Specific Multicast (SSM)
RFC3587	IPv6 Global Unicast Address Format
RFC4250–RFC4254	SSH server and client support

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
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 Monitoring (RMON)
RFC1907	SNMPv2
RFC1908	Coexistence between v1 & v2 of the Internet-standard Network Management Framework
RFC1930	Guidelines for creation, selection, and registration of an Autonomous System (AS)
RFC2541	Secure Shell Protocol Architecture
RFC2571	An Architecture for Describing SNMP Management Frameworks
RFC2572	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC2573	SNMP Applications
RFC2574	User-based Security Model (USM) for v3 of the Simple Network Management Protocol (SNMPv3)
RFC2575	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

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

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

Request for comment	Description
RFC2578	Structure of Management Information v2 (SMIv2)
RFC2674	Bridges with Traffic MIB
RFC2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC2863	Interface Group MIB
RFC2925	Remote Ping, Traceroute & Lookup Operations MIB
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 the 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

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
STDMIB4—Internet Assigned Numbers Authority (IANA) Interface Type	—	iana_if_type.mib
STDMIB5—Structure of Management Information (SMI)	RFC1155	rfc1155.mib
STDMIB6—Simple Network Management Protocol (SNMP)	RFC1157	rfc1157.mib
STDMIB7—MIB for network management of Transfer Control Protocol/Internet Protocol (TCP/IP) based Internet MIB2	RFC1213	rfc1213.mib
STDMIB8—A convention for defining traps for use with SNMP	RFC1215	rfc1215.mib
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

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
STDMIB17—Management Information Base of the Simple Network Management Protocol version 2 (SNMPv2)	RFC1907	rfc1907.mib
STDMIB21—Interfaces Group MIB using SMIv2	RFC2233	rfc2233.mib
STDMIB26a—An Architecture for Describing SNMP Management Frameworks	RFC2571	rfc2571.mib
STDMIB26b—Message Processing and Dispatching for the SNMP	RFC2572	rfc2572.mib
STDMIB26c—SNMP Applications	RFC2573	rfc2573.mib
STDMIB26d—User-based Security Model (USM) for version 3 of the SNMP	RFC2574	rfc2574.mib
STDMIB26e—View-based Access Control Model (VACM) for the SNMP	RFC2575	rfc2575.mib
STDMIB26f —Coexistence between Version 1, Version 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

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
STDMIB34—IPv4 Multicast Routing MIB	RFC2932	rfc2932.mib
STDMIB35—Internet Group Management Protocol MIB	RFC2933	rfc2933.mib
STDMIB36—Protocol Independent Multicast MIB for IPv4	RFC2934, RFC2936	rfc2934.mib, rfc2936.mib
STDMIB38—SNMPv3 These Request For Comments (RFC) make some previously named RFCs obsolete	RFC3411, RFC3412, RFC3413, RFC3414, RFC3415	rfc2571.mib, rfc2572.mib, rfc2573.mib, rfc2574.mib, rfc2575.mib
STDMIB39—Entity Sensor Management Information Base	RFC3433	
STDMIB40—The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model	RFC3826	rfc3826.mib
STDMIB41—Management Information Base for the 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 the 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
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

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 3.1.0.0 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 3.1.0.0.

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.

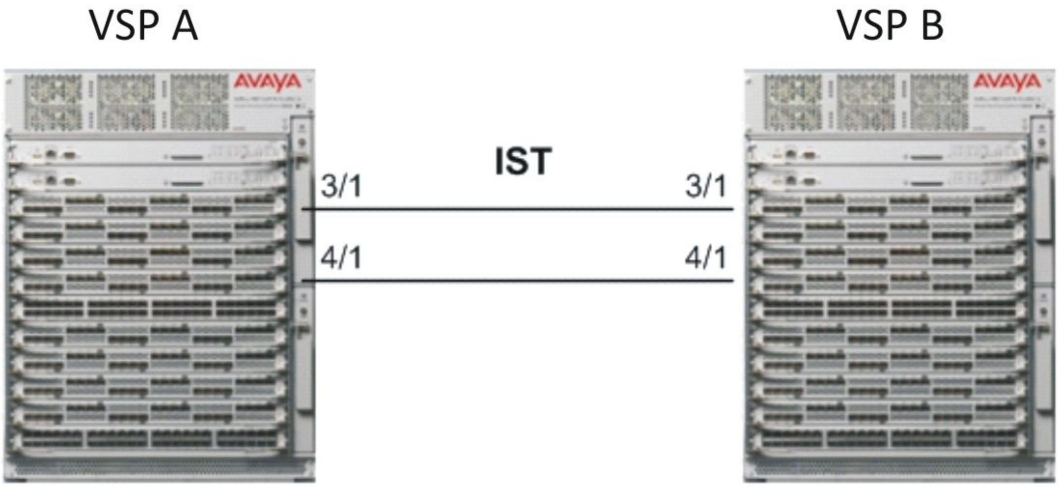

Figure 1: IST peer configuration

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.3.1.0.0.tgz
   software add-modules 3.1.0.0 VSP9K.3.1.0.0_modules.tgz
   ```
4. Activate the software release on both nodes of the cluster:

   ```
   software activate VSP9K.3.1.0.0
   ```
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 on page 45
- Interoperability issues on page 53
- Limitations on page 55

Known issues

The following table lists the known issues in Release 3.1 of the Avaya Virtual Services Platform 9000.

Table 23: Known issues

Issue number	Description	Workaround
Alarm / Logging / Error Reporting		
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 alarm logging file`** command to check the complete details and the CPU from which the alarm originated.
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.	
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	For the next KHI poll the CP will be up and will respond. This error message is not

Issue number	Description	Workaround
	sync error message appears.	service impacting and can be ignored.
wi00832713	VLACP can display an incorrect timestamp on the port up time.	Ignore the incorrect VLACP timestamps.
Bridging Functionality		
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.
Chassis Operations		
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.
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.	Telnet into the CP and redirect the alarm log to use internal flash.
wi00820546, wi00822103	The VSP 9000 does not support hot insert of multiple modules simultaneously in this release.	To insert multiple modules into a chassis, please insert and configure one module at a time.
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

Issue number	Description	Workaround
		TFTP, directly to the secondary CP.
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.	Increment the CP limit value by 200 packets per second.
EDM		
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`.	Click **OK** and logon the device again.
wi00565092	EDM supports Internet Explorer 7.0 and Mozilla Firefox 3.x. Use of other browsers, or other versions of supported browsers, may not offer full functionality or may not render the display as expected.	Use supported browsers to ensure full EDM functionality.
wi00668629	After deleting a VRF, all open EDM sessions that are using that VRF need to be closed manually by the user.	
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.	

Issue number	Description	Workaround
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.
wi00884199	You cannot open EDM Help files if you access the system over an HTTPS connection using Internet Explorer.	Use Mozilla Firefox or an HTTP connection.
wi00845679	You cannot modify, delete, or add the management IP address on the standby CP using EDM.	Use ACLI.
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.	Perform the OSPF-related configuration for the VLAN under the protocol itself instead of through the VLAN. For example, you can insert a new OSPF interface or modify existing OSPF interface parameters by using the **IP** > **OSPF** > **Interfaces** tab.
Management Access		
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.
wi00896935	FTP connections fail when the expected user authentication method is a configured RADIUS server.	A patch is available to resolve this issue. Contact Customer Support at http://www.avaya.com/support
MLT / SMLT		

Issue number	Description	Workaround
wi00510386	When all members of a MLT go down there is no trap generated.	Use the command **`show int gig state`** on all MLT member ports to display status.
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.
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 still 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.	
wi00885466	This issue occurs if you have a network with two VSP devices, VSP-A and VSP-B, in the core, that connect to an	

Issue number	Description	Workaround
	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.	
Multicast Operations		
–	The ACLI query-interval parameter for PIM interfaces and ports is changed to hello-interval. You can still use the query-interval parameter, but the configuration file saves this information as hello-interval and query-interval does not appear in ACLI Help text.	
Patching Operations		
wi00511642	The **`software patch commit`** and **`software patch remove`**	

Issue number	Description	Workaround
	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 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.	The remove command will not take effect until the commit is explicitly or automatically executed after a patch is reverted.
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.	
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.
Routing Operations		
wi00703966	There is a problem that can cause the standby CP to	

Issue number	Description	Workaround
	reboot during the synchronization of a large number of BGP routes from the master CP. If this does occur, the standby CP will reboot and attempt to synchronize with the master CP again. It will very likely synchronize correctly on the second attempt. During the time of standby CP reboot and resynchronization the traffic flow through the system is not effected because the master CP stays operational.	
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.	Configure IPv4 and IPv6 on different physical interfaces.
wi00886060	The ACLI command **`show ip vrrp interface`** does not show VRRP details for brouter ports.	Use **`show ip vrrp interface gigabitethernet`** to see 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.	Ignore the CLIP interfaces in the command output.
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.	Enable the required policy individually.

Issue number	Description	Workaround
wi00893530	If you delete an inter-VRF redistribution policy after an HA failover, the redistributed routes may not be removed from the forwarding table.	Check the routing table to confirm the routes are removed. If you observer stale entries, restart the protocol to remove the entries.
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.	This issue will be resolved in a future software release.
VLAN Operations		
wi00850312	If you delete the IPv6 address and IPv4 address from a VLAN interface, adding the IPv4 address again fails.	Do not configure both IPv4 and IPv6 addresses on the same VLAN interface.

Interoperability issues

The following table lists the known issues between Release 3.1 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 of the other Avaya product. Note that the issue will still exist in previous releases.

Table 24: 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.		

Issue number	Description	Workaround	Fixed in release
wi00521409	If you use one of the following interface modules in either slot 1 or slot 10 of an ERS 8600 with a slow backplane, the ERS does not receive the BPDUs the VSP 9000 sends, and both devices can become the root bridge: • 8630GBR • 8648GTR • 8683XLR	Do not use these modules in slot 1 or slot 10 of an ERS 8600 with a slow backplane. This is not a supported configuration.	
wi00565472	If you use one of the following interface modules in either slot 1 or slot 10 of an ERS 8600 with a slow backplane, unicast traffic from the VSP 9000 can be dropped on the ERS 8600 egress MLT port: • 8630GBR • 8648GTR • 8683XLR	Do not use these modules in slot 1 or slot 10 of an ERS 8600 with a slow backplane. This is not a supported configuration.	
wi00565499	If you use VSP and Ethernet Routing Switch 8600 on a VLAN, and all systems operate in MSTP mode, a loop can be generated if you restart a VLAN port on the Ethernet Routing Switch.	Disable the links on the Ethernet Routing Switch 8600 to remove the loop.	
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		

Issue number	Description	Workaround	Fixed in release
	VLACP packets from the VSP device. The VLACP link operational state is down.		
wi00691506	A topology change of an SMLT link between VSP 9000 systems and Ethernet Routing Switch 8600 Release 5.1.3 results in dropped packets. This problem occurs when one of the two MLT ports of the ERS is not a designated port or a root port. Topology changes make this port a blocking port and also other ports of the MLT change to the same state (blocking).		ERS 8600 5.1.4.0
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.	Disable and enable the port.	

Limitations

This section lists known limitations and expected behaviors that may first appear to be issues. The following table provides a description of the limitation or behavior and the work around, if one exists.

Table 25: 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	Use ACL-based filters to implement the MAC DA filter.

Issue number	Description	Workaround
	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.	The ACL-based filter works correctly regardless of whether the packet is bridged or routed.
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.

Chapter 8: Resolved issues

This section lists the issues resolved in Release 3.1.

Table 26: Resolved issues

Issue number	Issue description
Alarm/Logging/Error	
wi00866336	An IO module sends excessive log entries because of K2 event interrupts (log 17055e) and Zagros interface interrupts (log 17057d).
wi00876456	When you use the **`save config`** command, the `save to standby successful` alarm is seen even if no external flash is installed on the standby CP.
wi00881523	Some memory interfaces were not initialized properly causing RSP and K2 Errors on 9024XL modules.
wi00886798	If the system powers down a CP module, no alarm is raised and the module is no longer present if you use the **`show sys-info`** command.
Bridging Functionality	
wi00564393	When interworking with an ERS 8600 in RSTP mode, there can be a 30 second delay in packet forwarding due to a port role state transition mismatch between the VSP 9000 and the 8600.
wi00838325	Because of a port initialization issue on system reboot, sometimes RSTP ports may get stuck in a disabled state and never start forwarding traffic correctly.
Chassis Operations	
wi00732587	Intermittently swapping a 48 port SFP card with a 10 Gig 24 port card causes the standby CP to crash. There is no operational impact on traffic flow through the system but the system will be without a standby CP until the backup CP comes back online in about 4 minutes.
wi00825929	Although transmit flow control is disabled by default, if a port is shutdown and then enabled, the

Issue number	Issue description
	transmit and receive flow control values are overwritten. This happens on any port with auto-negotiation enabled. This is true for 1G SFPs on a 10G interface as well.
wi00830138	The ACLI command **`boot config host password`** does not synchronize to the hot standby CP. This can cause failures in copying files or saving PCAP files through FTP from the standby CP to the remote host.
wi00834423	Under rare circumstances on system startup, the internal compact flash device on the CP has shown mounting issues due to an intermittent hardware fault. When this occurs, all communications with the device are disabled and an error message is reported to the CP console. The CP will remain in this state until the card is power cycled and the hardware fault is reset. If the system runs in dual CP mode the second CP takes over mastership and generates the following hardware fault alarm: `0x00010738 00000000 GlobalRouter Critical error encountered for slot X error: HW fault prevents normal startup`. The only ill effect is that the startup process can take an additional 15 seconds to complete. In a single CP system, the only way to recover from this problem is to power cycle the chassis. Beginning with Software Release 3.0.2.0, you can use ACLI commands to identify the firmware version of the internal and external flash, and to backup and restore the flash. For more information about flash firmware versions with microcode errata and the replacement procedure, see *Avaya Virtual Services Platform 9000 Important Notice CP Module Compact Flash Replacement*, NN46250–108.
wi00838705	The following error message can appear on the console during system start: `LifeCycle: ERROR: Cannot create /opt/patch link patch`. This error is not critical and can be ignored.
wi00886784, wi00890924	When the backup CP module is taken offline by either the system or operator intervention, in most cases, the primary CP module would consider the backup dead and not allow the backup CP to come

Issue number	Issue description
	back online even after a replacement with a known good CP module.
wi00886793	The power down flag is not cleared after a CP module that has been powered down by the system is removed and reinserted.
EDM	
wi00826907	The EDM loop detection screen does not function as expected.
wi00830989	After configuring NLB-Mode in EDM on the **VLAN** > **Advanced** tab, a number is displayed instead of the values unicast or multicast. The displayed values correspond in the following way: 36–unicast, 18–multicast, 9–igmpMulticast
wi00831001	Internal VLAN 4092 and port 1/48 are some times displayed in the VLAN forwarding database table in EDM.
wi00831342	The IP domain name cannot be configured in EDM.
wi00831987	Static route weights cannot be configured in EDM.
wi00831436	When sorting multiple page listings in EDM by using the column header, only the first page of records sorts correctly.
wi00833659	When specifying the location of EDM help in the **Security** > **Control Path** > **General** screen, a valid HTTP port must be entered. Valid port values are between 80 and 49151. The port value will not be displayed after it has been saved.
wi00871917	VLAN names that include a slash ("/") cause errors when you try to modify VRRP parameters in EDM.
wi00873019	VLAN name changes made through ACLI do not take effect in EDM until after a browser restart.
wi00880636	In EDM when you assign a route policy to inter-VRF route redistribution with another VRF as the source VRF, you can configure inter-VRF route redistribution by global router only. However, route policy configuration is per VRF base, therefore you cannot view or change a policy you create in VRF x in another VRF.

Issue number	Issue description
wi00885035	A crash occurred while using EDM to access the internal flash on the remote CP module when it was unoperational.
Various	Context sensitive help is not available for all VSP 9000-related COM and EDM screens. All monitoring and configuration procedures can also be found in the documentation for the specific features. See *Avaya Virtual Services Platform 9000 Documentation Roadmap* , NN46250-100 to locate information for a particular feature.
Filtering	
wi00826461	Global actions are applied even if a packet does not match any of the ACEs.
HA Operations	
wi00727269	On a warm standby device, pulling the active CP results in the device rebooting two times after it fails over to the warm standby CP.
IST Operations	
wi00732505	The sequence of how loop-detect is configured on IST ports is important. Once you configure an IST, you cannot configure loop-detect on that port. If you already had loop-detect configured on the port before making it an IST port, the system does not prevent this error condition from happening. Do not add ports to an IST that already has loop-detect enabled.
wi00859221	This fix prevents the IST protocol from establishing a connection between a VSP 9000 that runs Release 3.0.0.0 and a VSP 9000 that runs Release 3.1.0.0. When you upgrade a pair of VSP 9000 core switches that connect through an IST peer connection, note that the IST channel will be down for the duration of the upgrade procedure. See Upgrading IST peer switches on page 41 for instructions about how to minimize the network downtime.
Management Access	
wi00832793	CP crash can occur if you issue continuous SNMP gets at a high rate.
wi00833216	A telnet session to the standby CP is not forcefully logged out when a CP switchover occurs.

Issue number	Issue description
wi00850672	Telnet sessions may not time out if left at a prompt requiring input, resulting in ACLI console lockup.
wi00868956	The -y option to delete files does not work as expected. You are prompted for confirmation of each file rather than deleting all files without confirmation.
wi00869501	After an SSH session is logged out, a crash can occur when you initiate a new SSH session.
wi00871967	Multiple Telnet sessions to the virtual management IP address will become unresponsive after several days and no new Telnet sessions can be established.
wi00873312	If SSH sessions are terminated by using the SSH application itself, for example, by pressing the **disconnect** button on SecureCRT or the equivalent on EDM, rather than typing the ACLI command **`exit`**, eventually no more SSH sessions using ACLI can be established.
wi00884979	The Telnet connection to the management virtual IP address becomes unreachable if the management port on either of the CP modules goes down or is bounced.
wi00889008	A CP crash can occur while applying an access policy within an SSH session, specifically denying the current SSH session.
MLT/SMLT	
wi00825953	Unexpected console messages may be encountered during boot on devices in a full mesh SMLT configuration with LACP enabled. These console messages can generally be ignored as they do not pertain to the configuration or any failure in it.
Multicast Operations	
wi00829738	The command `no ip pim fast-joinprune` also disables PIM globally.
wi00833276	Multicast traffic is lost for about 5 minutes in a single port IST setup when the square SMLT link is down.
wi00851789	Corruption in the IP multicast table caused the IO module to crash during tables updates.
Routing Operations	

Issue number	Issue description
wi00823867	The IPv6 virtual management address is shown in two places in the output of the **`show running-config`** command. One is under `MGMT VIRTUAL IP CONFIGURATION` and the other is under `IPv6 MGMT INTERFACE CONFIGUATION`.
wi00870101	The VSP removes StaticARP of a device when the device renews the IP address lease by sending DHCP Request.
wi00870742	After a broadcast DHCPRENEW packet was received by the relay agent, the dynamic ARP entry was removed, requiring the client to send an ARP request again.
wi00877787	An OSPF crash can occur if you use IP supernet over VRF.
wi00880069	The secondary CPU crashes when you configure route policies to filter routes redistributed between VRFs.
wi00880625	ARP entries are not removed after an ARP request times out and a static route exists with a next hop that is dependent on the ARP entry.
wi00884557	As part of route redistribution between VRFs, directly connected interfaces from the source VRF were not populated in the data-path, causing packets to these destinations to go to the CPU.
System Operations	
wi00834419	If an upgrade hangs during the reboot phase, the commit timer can still fire, which causes the auto-commit to still take effect.
wi00866330	A delay exists in writing the backtrace to the flash. which can result in the backtrace not being saved.
wi00866333	The CP module can be reset while writing a core dump, which results in an incomplete core dump file.
Statistics Reporting	
wi00511487	EAPoL session statistics for a particular port are not collected or displayed.
wi00520783	Multicast statistics on IST ports include LSM (Link State Message) packets which update peer port state information.

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.

Navigation

- Getting technical documentation on page 63
- Getting product training on page 63
- Getting help from a distributor or reseller on page 63
- Getting technical support from the Avaya Web site on page 64

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.

Index