Release Notes — Release 3.0
Avaya Virtual Services Platform 9000

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 3.0:

- Features on page 5
- Other changes on page 5

Features

There are no feature changes.

Other changes

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

Open Source software

The filenames for Open Source software are updated. For more information, see File names for this release on page 17.

New in this release

Chapter 2: Introduction

This document describes the features and known issues of the Avaya Virtual Services Platform 9000 Release 3.0. Use this document to help you optimize the functionality of your device.

Avaya Virtual Enterprise Network Architecture (VENA) expands Avaya's proven 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 Release 3.0 and provides important information for this release.

New hardware

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

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 9080CP module comes with a slot for a CPx daughtercard and a Hard Disk (HD) controller card for future use.

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

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 Control Processor 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 they are placed. The SF slots 1 and 4 are for system operations and are called bandwidth managers. At least one SF module in slots 1 and 4 must operate at all times for the interface modules to send traffic to the fabrics. You must install a minimum of four SF modules in the chassis.

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 managers
SF2, SF3, SF5, and SF6	X-bar functions

The 9090SF modules can provide the following maximum throughput for each interface module:

- 70 Gbps throughput for each 9024XL

- 46 Gbps throughput for each 9048GT or 9048GB

9012SC Switch Fabric cooling module

The 9012SC Switch Fabric (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 line rate of more than 100Mpps over 24 ports of 10 Gb/s Ethernet traffic using standard SFP+ fiber connectors. The module supports Short Range (SR) and Long Range (LR) 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. It has a maximum throughput of 105 Mpps.

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. It 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. It has a maximum throughput of 70 Mpps.

New features

Layer 1

  9k Jumbo packet support

Layer 2

- Port, Source MAC, IP subnet, and Protocol-based VLANs
- IEEE 802.1D Mac Bridges / Spanning Tree
- IEEE 802.1w/s RSTP / MSTP
- IEEE 802.1p/Q Virtual LAN
- IEEE 802.3x Flow control (RX enabled / TX disabled)
- MLT / SMLT
- IEEE 802.1AX Link Aggregation
- VLACP End-to-End connectivity check
- Simple Loop Prevention Protocol (SLPP)

Packet Classification

- Diffser framework
- Ingress port and flow policers
- Egress port shapers

Layer 3 Internet Protocol Suite

- Port features

    Brouter port

- Link Layer

    ARP, RARP

- Internet Layer

    - IP (& ECMP)

    - ICMP

- Transport Layer

    TCP, UDP

- Application Layer

    - VRRP

    - DHCP, DHCP Relay

    - Static routes

    - RIP

    - OSPF

    - BGP

    - FTP, TFTP, HTTP, SNMPv1,v2,v3, SSH, Telnet

- Multicast

    - IGMPv2 / v3

    - PIM-SM / SSM

IPv6

- IPv6 Management SNMP, Telnet, Ping
- IPv6 MLDv1 Host (RFC 2710) & MLDv2 Host (RFC 3810)

Network Virtualization Services

- VRF (512 instances)
- Virtualized: OSPF, RIP, VRRP, Route policies, DHCP Relay, Ping

Serviceability

- Flight Recorder for system health monitoring
- Debugging, Logging
- Filter logging
- Online Packet Capture (PCAP)
- Hitless patching

Management

- Enterprise Device Manager (EDM)
- Unified Communication Manager (UCM)
- Common Orchestration Manager (COM)
- ACLI
- SNMPv1,2 & 3
- Licensing Infrastructure
- Port-, Flow-, Remote for port and flow ingress and egress Mirroring
- IPv6 Management SNMP, Telnet, Ping
- Route Policies
- RADIUS

Resiliency

- Switch Clustering: SMLT / RSMLT / RSMLT-edge / MSMLT
- High Availability Mode (HA L2 & L3)
- VRRP, VRRP-BackupMaster
- Port / Link / Route Rapid Failure Detection and Recovery (RFDR)
- Hardware-based CP protection

Security

- Control Plane DOS protection
- Line Rate Ingress and Egress Port & VLAN ACLs for L2 to L4
- 16k filter rules
- Access control features
- EAP
- Reversepath Forwarding Check

File names for this release

This section describes the Avaya Virtual Services Platform 9000 Release 3.0 software files.

Release 3.0 software files

The following table gives the details of the Virtual Services Platform 9000 Release 3.0 software files.

Table 6: Release 3.0 software files

File name	Description	Size
vsp9k3.0.0.0.tgz	Release 3.0 archived distribution	90 MB

Release 3.0 Open Source software files

The following table gives the details of the Open Source software files distributed with the Virtual Services Platform 9000 Release 3.0 software.

Table 7: Release 3.0 Open Source software files

File name	Description	Size
VSP9K.3.0.0.0_Copyright.mht	Master copyright file.	351 KB

File name	Description	Size
VSP9K.3.0.0.0_OpenSource.zip	Open source base software for Virtual Services Platform 9000 Release 3.0.	302 MB

All Avaya Virtual Services Platform 9000 Release 3.0 software and files can be downloaded from the Avaya Support Portal at http://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 Release 3.0.

Protecting modules

⚠️ **Caution:**

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

✴️ **Note:**

If you have the optional external Flash card media for your CPU module, you must install it prior to power on of the Chassis and CPU modules.

⚠️ **Caution:**

Modules are heavy. Damage to a module can occur if it's bumped 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 a module's connectors against an adjacent module's ejector levers. Damage to connectors may result.

Supported browsers

The following browsers are supported for accessing the Enterprise Device Manager (EDM) on the Virtual Services Platform 9000:

- Microsoft Internet Explorer 7.0
- Mozilla Firefox 3.0 and above

Environmental specifications

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

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
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
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
Fabric Switch module	300 000 hours

Component	Mean time between failures
Control Processor module	250 000 hours
Interface modules	200 000 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.
- The installer 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

Release 3.0 of the Virtual Services Platform 9000 does not support user configurable SSL certificates.

EDM image management

EDM does not currently support image management functionality. All image management work must be performed through the ACLI. This includes, but is not limited to, software upgrades, software image management, and software patching. Refer to *Avaya Virtual Services Platform 9000 Upgrades and Patches — Software Release 3.0* (NN46250–400) for information and procedures pertaining to these work areas.

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

Chassis, switching fabrics, and control processors		Minimum software version	Part number
9080CP	Control Processor module	3.0	EC1404007-E6
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)

Chassis, switching fabrics, and control processors			Minimum software version	Part number
				AA1419077-E6 (40 km at 1490 nm)
	1000BASE-EX DDI SFP	1550 nm, Gigabit Ethernet, duplex LC connector	3.0	AA1419071-E6
	1000BASE DDI CWDM 40 km SFP	Gigabit Ethernet, duplex LC connector	3.0	AA1419053-E6 to AA1419060-E6.
	1000BASE DDI CWDM 70 km SFP	Gigabit Ethernet, duplex LC connector	3.0	AA1419061-E6 to 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

This section lists hardware scaling capabilities of the Avaya Virtual Services Platform 9000 Release 3.0.

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 speed	1.33 GHz
9012 Chassis	
Control Processor (CP) modules	2
Console port	1 D-subminiature 25-pin shell 9 pin connector (DB9)

	Maximum number supported
Ethernet management	1 Registered Jack (RJ) 45
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 4 SF modules in the chassis.
Lights out Management 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 Release 3.0.

Table 15: Software scaling capabilities

	Maximum number supported
Layer 2	
IEEE/Port-based VLANs	4084
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

	Maximum number supported
S/MLT Ports per group	16
LACP	512 aggregators
LACP ports per aggregator	8 active and 8 standby
VLACP Interfaces	128
SLPP	500 VLANs
Layer 3	
Internet Protocol version 4 (IPv4) Interfaces	4343
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	2048 for each VRF, 10K for each system
Static routes (IPv4)	2000 per 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 per VRF)
RIP interfaces	200
RIP routes	2500 for each VRF, maximum of 10K per system
OSPF instances	64 (one per VRF)
OSPF interfaces	512 active, 2000 passive
Open Shortest Path First (OSPF) adjacencies	512
OSPF areas	12 per OSPF instance, 80 per system
OSPF LSA packet size	Jumbo packets
OSPF routes	64 000
BGP peers	256
BGP Internet peers (full)	3
BGP routes	1.5 million

	Maximum number supported
IP Routing policies (IPv4)	500 per VRF, 5000 per system
IP Prefix List	500
IP Prefix entries	25 000
RSMLT interfaces	4000 over 128 SMLT interfaces
Multicast IGMP interfaces	4084
Multicast source and group (S, G)	4000
PIM interfaces	512 active; 4084 passive
VRRP interfaces	256 per VRF / 512 per system
VRRP interfaces fast timers (200ms)	24
UDP/DHCP Forwarding entries	512 per VRF / 1024 per system
NLB Clusters — Unicast	128 per VLAN / 2000 per system
NLB Clusters — Multicast	1 per VLAN / 2000 per 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	2048
Access Control Entries (ACE) for each chassis	16 000
ACEs per ACL (any combination of Security and QoS ACEs)	1000
Unique Redirect Next Hop Values for ACE Actions	2000
Diagnostics	
Mirrored ports	479
Remote Mirroring Termination (RMT) ports	32

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)
802.3ad	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)
802.1X	Extended Authentication Protocol (EAP), and EAP over LAN (EAPoL)

Supported RFCs

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

Table 17: Supported request for comments

Request for comment	Description
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
RFC1541 and RFC1542, updated by RFC2131	Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) protocols
RFC1812	Router requirements
RFC1866	HyperText Markup Language version 2 (HTMLv2) protocol
RFC2068	Hypertext Transfer Protocol

Standard MIBs

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

Table 18: Supported MIBs

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
STDMIB2— Link Aggregation Control Protocol (LACP) (802.3ad)	802.3ad	ieee802-lag.mib
STDMIB3—Exensible Authentication Protocol Over Local Area Networks (EAPoL) (802.1x)	802.1x	ieee8021x.mib
STDMIB4—Internet Assigned Numbers Authority (IANA) Interface Type	—	iana_if_type.mib
STDMIB5—Structure of Management Information (SMI)	RFC1155	rfc1155.mib
STDMIB6—Simple Network Management Protocol (SNMP)	RFC1157	rfc1157.mib
STDMIB7—MIB for network management of Transfer Control Protocol/Internet Protocol (TCP/IP) based Internet MIB2	RFC1213	rfc1213.mib
STDMIB8—A convention for defining traps for use with SNMP	RFC1215	rfc1215.mib
STDMIB9—Routing Information Protocol (RIP) version 2 MIB extensions	RFC1389	rfc1389.mib
STDMIB10—Definitions of Managed Objects for Bridges	RFC1493	rfc1493.mib
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	RFC1657	rfc1657.mib

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
Gateway Protocol (BGP-4) using SMIv2		
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 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

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
STDMIB31—Textual Conventions for Internet Network Addresses	RFC2851	rfc2851.mib
STDMIB32—The Interface Group MIB	RFC2863	rfc2863.mib
STDMIB33—Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations	RFC2925	rfc2925.mib
STDMIB34—IPv4 Multicast Routing MIB	RFC2932	rfc2932.mib
STDMIB35—Internet Group Management Protocol MIB	RFC2933	rfc2933.mib
STDMIB36—Protocol Independent Multicast MIB for IPv4	RFC2934, RFC2936	rfc2934.mib, rfc2936.mib
STDMIB38—SNMPv3 These Request For Comments (RFC) make some previously named RFCs obsolete	RFC3411, RFC3412, RFC3413, RFC3414, RFC3415	rfc2571.mib, rfc2572.mib, rfc2573.mib, rfc2574.mib, rfc2575.mib
STDMIB39—Entity Sensor Management Information Base	RFC3433	
STDMIB40—The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model	RFC3826	rfc3826.mib
STDMIB41—Management Information Base for the 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 19: 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: Updating the Software Image and Verifying the Software Load

The software provided with a new Avaya Virtual Services Platform 9000 device contains minimal functionality and is not intended for a production environment. Refer to *Avaya Virtual Services Platform 9000 Commissioning* (NN46250-300) for information on upgrading to the latest software release. Use the ACLI command `show software details` to verify the upgraded software. The output displayed below is an example of a Virtual Services Platform 9000 running production software. The output of the command on your system should be similar.

```
VSP-9012:1#show software detail

================================================================================
                      software releases in /intflash/release/
================================================================================
3.0.0.0.GA (Primary Release)
  MP
    UBOOT                           int22
    KERNEL                          dev_int30
    ROOTFS                          int281
    APPFS                           VSP9K.3.0.0.0int327
  IOP
    UBOOT                           int22
    KERNEL                          dev_int30
    ROOTFS                          int281
    APPFS                           VSP9K.3.0.0.0int327
  IO_24PORT
    UBOOT                           int22
    KERNEL                          dev_int30
    ROOTFS                          int281
    APPFS                           VSP9K.3.0.0.0int327
  IO_48PORT
    UBOOT                           int22
    KERNEL                          dev_int30
    ROOTFS                          int281
    APPFS                           VSP9K.3.0.0.0int327
  SF
    UBOOT                           int22
    KERNEL                          dev_int30
    ROOTFS                          int281
    APPFS                           VSP9K.3.0.0.0int327
  FPGA
    OXIDE                           10040918
    PHOSPHIDE                       10041310
    CATSKILL                        10052013
    ZAGROS                          10101216
    SULPHIDE                        10041310
    K2                              10052408
  AVAILABLE ENCRYPTION MODULES
    AES
    DES/3DES
```

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 section lists the known issues in Release 3.0 of the Avaya Virtual Services Platform 9000.

Table 20: Known issues

WI	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.
wi00832713	VLACP may display an incorrect timestamp on the port up time.	Ignore the incorrect VLACP timestamps.
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.	
Bridging Functionality		
wi00511527	MSTP bridges may not learn the correct CIST regional root.	If this problem is encountered the operator can change the bridging

WI	Description	Workaround
		priority of the switch to make sure the root selection occurs as desired.
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.	Running the bridged network in MSTP mode is the most effect remedy for this problem.
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.
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.	The operator can disable then re-enable Spanning Tree on the effected RSTP ports to correct the problem.
Chassis Operations		
wi00731983	If the external compact flash card is removed from the chassis after it is booted, 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.
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	The operator can detect this fault condition by the console output from the failed CP or via telnet or console access to the backup CP. When the failure is detected the operator can power cycle the failed CP to force a reset of the compact flash device. This will clear up the problem.

WI	Description	Workaround
	state until the card is power cycled and the hardware fault is reset. If the system is running in dual CP mode the second CP will take over mastership and generate 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 boot up process could take an additional 15 second to complete. In a single CP system the only way to recover from this problem is to power cycle the chassis.	
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.	
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.
wi00820546, wi00822103	The VSP 9000 does not support hot insert of multiple	To insert multiple modules into a chassis, please insert

WI	Description	Workaround
	modules simultaneously in this release.	and configure one module at a time.
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.	To workaround this problem, use the command `boot config host user` after you use `boot config host password`. The configuration of `boot config host user` synchronizes both the user name and password to the host standby CP.
wi00825929	Although transmit flow control is disabled by default, if a port is shutdown and then enabled, the 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.	To work around this problem enable and then disable transmit flow control on the port so that the flow control values are reset on the interface.
wi00838705	The following error message may be displayed on the console during system boot: `LifeCycle: ERROR: Cannot create /opt/ patch link patch`. This error is not critical and can be ignored by the operator.	Simply ignore this error message as it has no effect on system operations.
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	Use supported browsers to ensure full EDM functionality.

WI	Description	Workaround
	may not render the display as expected.	
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.	
wi00820028	The operator 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 may 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.
wi00825617	EDM may display port 1/48 in the VLAN forwarding table.	This port is shown in error and can be ignored.
wi00831342	The IP domain name cannot be configured in EDM.	Use ACLI to configure the IP domain name as necessary.
wi00831987	Static route weights cannot be configured in EDM.	Use ACLI to configure static route weights as necessary.
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.	
wi00826907	The EDM loop detection screen does not function as expected.	

WI	Description	Workaround
wi00830411	Error messages may be displayed on the console when connected to EDM using Internet Explorer 6.0. Internet Explorer 6.0 is not supported.	Discontinuing use of this browser will discontinue the error messages.
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.	Ignore these display errors.
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. Refer to the *Avaya VSP 9000 Documentation Roadmap* (NN46250-100) to locate information for a particular feature.	
Filtering		
wi00664833	The MAC DA filter is only applicable for traffic that is being bridged through the device. If the packet is being routed, then the legacy MAC DA filter is not applied for traffic that is being routed through the box.	Use ACL-based filters to implement the MAC DA filter. The ACL-based filter will work correctly regardless of whether the packet will be bridged or routed.
wi00826461	Global actions are applied even if a packet does not match any of the ACEs.	

WI	Description	Workaround
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.	
Interoperability		
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.	
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	
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	
wi00565499	If you use VSP and Ethernet Routing Switch 8600 on a VLAN, and all systems operate in MSTP mode, a	Disable the links on the Ethernet Routing Switch 8600 to remove the loop.

WI	Description	Workaround
	loop can be generated if you restart a VLAN port on the Ethernet Routing Switch.	
wi00689238	If a VSP 9000 aggregation switch sends a high volume (more than 3000) of OSPF or RIP routes to an Ethernet Routing Switch 8600 edge device to redistribute into an OSPF domain, the CPU utilization of the edge device can increase, which results in dropping all VLACP packets from the VSP device. The VLACP link operational state is down.	
wi00691506	A topology change of an SMLT link between VSP 9000 systems and Ethernet Routing Switch 8600 Release 5.1.3 results in dropped packets. This problem occurs when one of the two MLT ports of the ERS is not a designated port or a root port. Topology changes make this port a blocking port and also other ports of the MLT change to the same state (blocking).	
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.
Management Access		
wi00510551	Compression options are not supported in SSHv2 but no	Do not use compression options with SSHv2.

WI	Description	Workaround
	error message is displayed when they are used.	
wi00509904	File transfer may fail when attempting to move large files with TFTP.	Use FTP for transfer of files larger than 32MB.
wi00520113	Transferring files using passive FTP may fail when using a Windows PC.	Use active mode when transferring files with FTP.
wi00833216	A telnet session to the standby CP is not forcefully logged out when a CP switchover occurs.	The operator should log out of the standby CP after a CP switchover occurs.
MLT / SMLT		
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.
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.
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.
wi00822560	Disable member ports before deleting an MLT.	
Multicast Operations		
wi00829738	The command `no ip pim fast-joinprune` also disables PIM globally.	Be aware of this fact and plan your configuration steps accordingly.
wi00833276	Multicast traffic is lost for about 5 minutes in a single port IST setup when the square SMLT link is down.	Configure 2 or more IST links as stated in Avaya recommended guidelines.
Patching Operations		
wi00511642	The `software patch commit` and `software`	

WI	Description	Workaround
	`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 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.
Quality of Service (QoS)		
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.	
Routing Operations		
wi00703966	There is a problem that may cause the standby CP to reboot during the synchronization of a large number of BGP routes from	

WI	Description	Workaround
	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.
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`.	This problem has no impact on functionality. An error is displayed in the log indicating that the address already exists with no harmful side effects.
Statistics Reporting		
wi00511487	EAPoL session statistics for a particular port are not collected or displayed.	Statistics for the inband-port can be obtained using the `show interface gigabitEthernet statistics` command.
wi00520783	Multicast statistics on IST ports include LSM (Link State Message) packets which update peer port state information.	Use the `show routing statistics interface` command for details about your multicast traffic.

Chapter 8: 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

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