Release Notes for Avaya Virtual Services Platform 8200

Release 4.1
NN47227-401
Issue 04.02
March 2015

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

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

Licence types

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

Heritage Nortel Software

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

Copyright

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

Third Party Components

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

Preventing Toll Fraud

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

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

This document describes important information about this release of the VSP 8284XSQ product. The VSP 8284XSQ is a member of the Avaya Virtual Services Platform 8000 Series. This is a new family of high-performance Ethernet Switches developed by Avaya.

The Virtual Services Platform 8200 Series is a sub-family of compact fixed form factor switches in the Virtual Services Platform 8000 Series. The VSP 8284XSQ is the first switch model in this series to be released.

These Release Notes include supported hardware and software, scaling capabilities, and a list of known issues (including workarounds where appropriate). This document also describes known limitations and restrictions.

Related resources

Documentation

See the *Documentation Reference for Avaya Virtual Services Platform 8200,* NN47227-100 for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com/.

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Subscribing to e-notifications

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

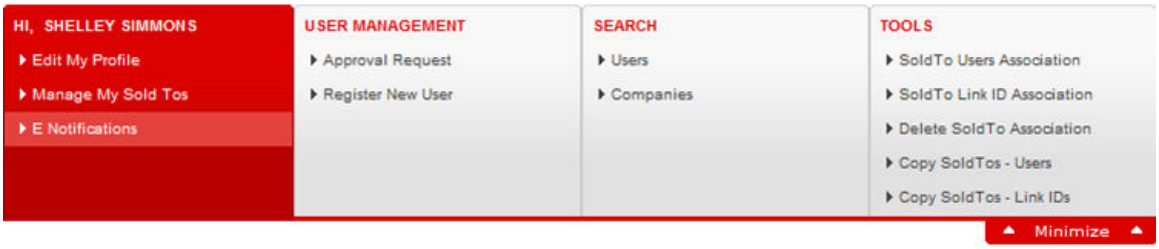
About this task

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

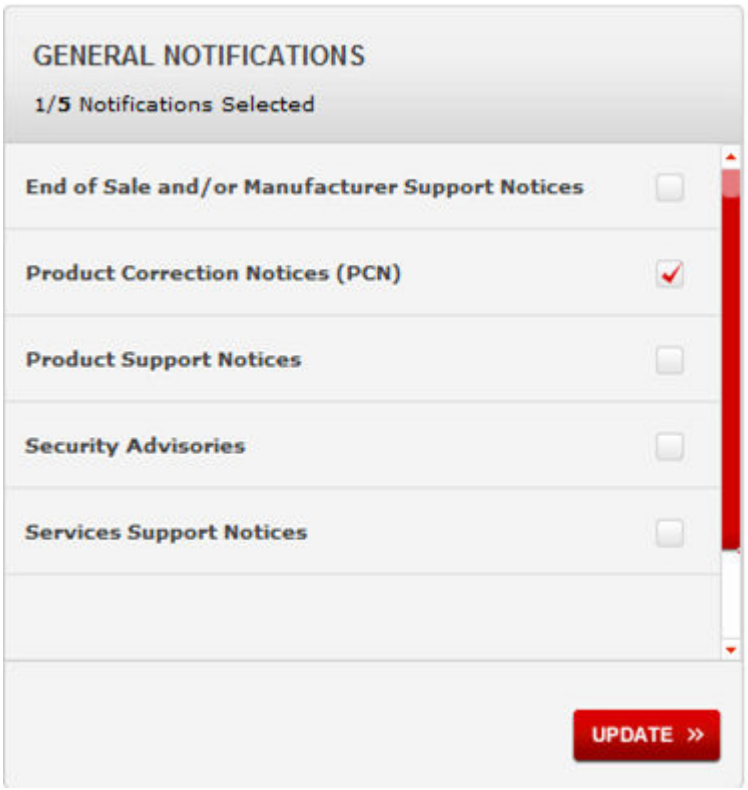
Procedure

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

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

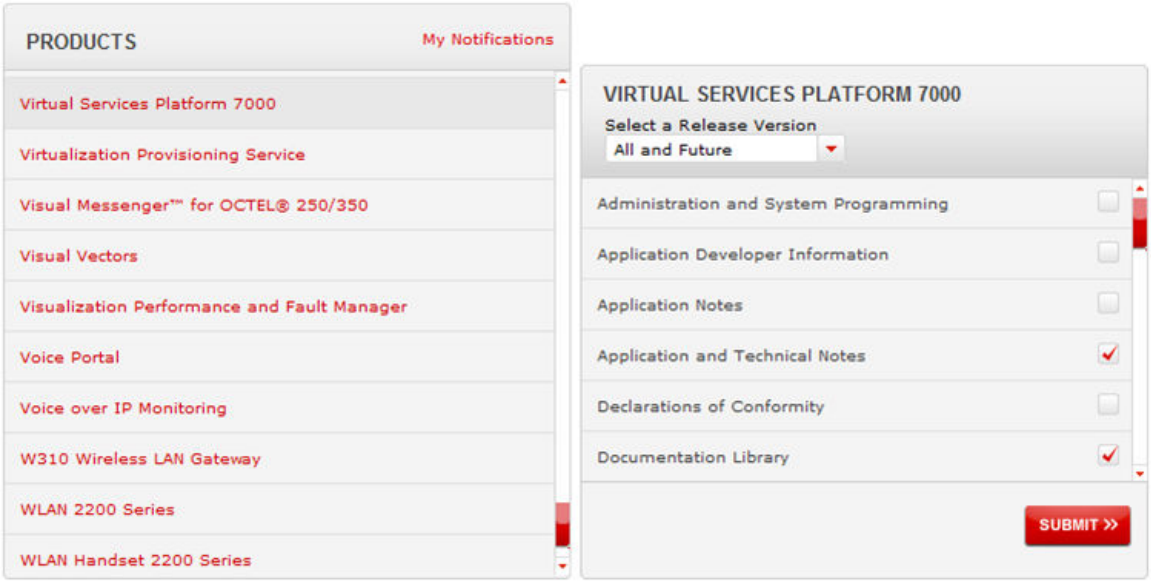


5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.



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

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



11. Click **Submit**.

Support

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

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx.

3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
   - Whole Words Only
   - Case-Sensitive
   - Include Bookmarks
   - Include Comments
6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Chapter 2: New in this release

The following sections detail what is new in *Release Notes for Avaya Virtual Services Platform 8284XSQ,* NN47227-401 for Release 4.1.

Features

See the following sections for information about feature changes.

IPv6

Release 4.1 introduces support for IPv6 routing.

Base IPv6 features:

- Dual-Stack IPv4/IPv6 support
- 6in4 Configured Tunnels to enable transition from IPv4 to IPv6 networks
- IPv6 Routing (Static, OSPFv3)
- Resilient IPv6 network design enabled by VRRPv3 and IPv6 support on SMLT/RSMLT links
- IPv6 connectivity for management protocols to enable RADIUSv6, DHCPv6, DNSv6 and Syslog servers in IPv6 network
- IPv6 OAM support including Ping, Traceroute, Telnet, FTP, TFTP, Rlogin, SSH, SNMPv3, EDM access via IPv6 HTTPS
- IPv6 Access Control Lists (ACLs)

Note:

The software does not support IPv4-mapped IPv6 addresses, for example, 0::FFFF:a.b.c.d, or IPv4-compatible IPv6 addresses, for example, 0::a.b.c.d.

IPv6 over Fabric:

- IPv6 Shortcuts
- IPv6 routing between Layer 2 VSNs

For more information, see *Configuring IPv6 Routing on Avaya Virtual Services Platform 8200,* NN47227–507.

IPv6 Access Control Lists (ACLs)

Release 4.1 adds support for IPv6 ingress port/vlan security ACL/Filters. VSP 8200 supports a maximum of 256 IPv6 ingress port/vlan security ACL/Filters. IPv6 ingress QoS ACL/Filters and IPv6

egress security and QoS ACL/Filters are not supported. For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8200,* NN47227-502.

IPv6 Shortcuts

Release 4.1 adds support for IPv6 Shortcuts, which function in a very similar manner to IPv4 Shortcuts. Both types of Shortcuts use IS-IS as the Interior Gateway Protocol (IGP) and the link-state packet (LSP) for reachability information. However, IPv4 Shortcuts use TLV 135 and IPv6 Shortcuts use TLV 236. All TLVs announced in the IS-IS LSPs are grafted onto the shortest path tree (SPT) as leaf nodes.

IPv6 Shortcuts use some IPv4 Shortcuts functionality so IPv4 Shortcuts must be enabled before you enable IPv6 Shortcuts. For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.

IPv6 Routing between Layer 2 VSNs

IPv6 routing between Layer 2 VSNs (Inter-VSN routing) allows configuration of any SPB IPv6 capable node to also provide Inter-ISID Layer 2 VSN routing by adding an IPv6 interface to a port-less CVLAN. IPv6 Unicast traffic can then be routed anywhere in the SPB fabric on SPB-IPv6 capable nodes.

Inter-VSN routing with SPBM allows routing between Layer 2 VLANs with different I-SIDs. For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.

Layer 3 VSN

Release 4.1 adds support for the Layer 3 Virtual Services Network (VSN) feature. The Layer 3 VSN feature provides IP connectivity over SPBM for VRFs. Layer 3 VSNs use IS-IS to exchange the routing information for each VRF.

Note:

Layer 3 VSN is supported only for IPv4

For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.

eBGP

Release 4.1 introduces support for Border Gateway Protocol (BGP), which is an inter-domain routing protocol that provides loop-free routing between autonomous systems (AS) or within an AS. In this release, the following operations are supported by BGP:

- IPv4
- 4–byte AS
- Peer groups
- Redistribution

Note:

This release does not support iBGP, BGP+, BGP Confederations, and BGP Route Reflectors.

For more information, see *Configuring BGP Services on Avaya Virtual Services Platform 8200,* NN47227–508.

IP Multicast over SBPM

Release 4.1 supports IP multicast over Shortest Path Bridging MAC (SPBM). IP multicast over SPBM greatly simplifies multicast deployment, with no need for any multicast routing protocols such as PIM.

With IP multicast over SPBM, Avaya leads the industry with a new approach to transport IP multicast. SPBM uses Intermediate-System-to-Intermediate-System (IS-IS) as the control plane and relies on a Shortest Path Tree (SPT) on every switch to transport data across the Virtual Services Fabric. The Backbone Edge Bridge (BEB) can forward a multicast stream anywhere in an SPBM network where IS-IS advertises the stream to the rest of the fabric.

For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.

Intermediate-System-to-Intermediate-System (IS-IS) accept policies

Release 4.1 adds Intermediate-System-to-Intermediate-System (IS-IS) accept policies. You can use IS-IS accept policies with Layer 3 VSNs or IP Shortcuts to filter incoming IS-IS routes over the SPBM cloud. IS-IS accept policies enable the device to determine whether to add an incoming route to the routing table. IS-IS policies can also use either a service instance identifier (I-SID) or an I-SID list to filter incoming traffic.

For information on how to configure IS-IS accept policy filters, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.

E-Tree and Private VLANs

Private VLANs consist of a primary and a secondary VLAN that provide isolation between ports within a Layer 2 service. The E-Tree feature allows private VLANs to traverse an SPBM network by associating a private VLAN with an I-SID.

- For more information about E-Tree, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.
- For more information about private VLANs, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 8200,* NN47227-500.
- For information about configuring MultiLink Trunks (MLT) and Private VLANs, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8200,* NN47227-503.

EAPoL IEEE 802.1x–2001

Release 4.1 supports IEEE 802.1x based Extensible Authentication Protocol over LAN (EAPoL).

EAPoL is a port-based network access control protocol. EAPoL provides security by preventing users from accessing network resources before they are authenticated. The EAPoL authentication feature prevents users from accessing a network to assume a valid identity and access confidential material or launch denial-of-service attacks.

For more information, see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.

MACsec

Release 4.1 introduces support for Media Access Control Security (MACsec) to provide Layer 2 security for connections between core switches or core and edge switches where cabling infrastructure is external to both offices. The ability to use MACsec in this situation provides a high

level of security without acquiring third-party encryption platforms. For more information, see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.

Service Level Agreement Monitor

Release 4.1 adds support for the SLA Mon™ agent. You can use SLA Mon to monitor and analyze performance issues in the network infrastructure.

For more information, see *Monitoring Performance on Avaya Virtual Services Platform 8200,* NN47227-701.

TACACS+

Release 4.1 supports the Terminal Access Controller Access Control System Plus (TACACS+) client. TACACS+ is a client and server-based protocol that provides centralized validation of users who attempt to gain access to a router. For more information see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.

SPBM install script

Release 4.1 supports an ACLI script to quickly enable Avaya VENA Fabric Connect on a switch. You can use the command **`run spbm`** to quickly set up the SPB and IS-IS configuration.

The **`run spbm`** command enables you to modify the default parameters. The console displays each parameter with the default value in brackets, which you can modify by entering another value.

For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.

VLACP statistics

Release 4.1 adds the ability to enable sequence numbers for VLACP PDUs to assist with monitoring dropped packets. New commands also enable you to display and clear VLACP statistics. For more information see *Monitoring Performance on Avaya Virtual Services Platform 8200,* NN47227-701.

Licensing support

Starting with Release 4.1, Avaya Networking is moving to Product Licensing & Delivery System (PLDS) as the license order, delivery and management tool. PLDS provides self-service license activations, upgrades, moves/changes.

Release 4.1 introduces licensing on the VSP 8000 platform with a premier license being required for L3 VSNs and MACsec features.

There are two types of Premier licenses:

- Support for Layer 3 VSNs only
- Support for Layer 3 VSNs and MACsec

All other features that are part of 4.1 are not licensed.

For customers that would like to trial premier features prior to purchasing a premier license, there are there are two types of PLDS Premier trial licenses that will permit use of premier features for a 60 day period:

- Support for Layer 3 VSNs only
- Support for Layer 3 VSNs and MACsec

The PLDS Premier trial license is generated using the system MAC address of a switch and can only be generated and used once for a given MAC address. After the expiry of the 60 day trial

period, you will see messages on the console and in the alarms database that the license has expired. If you restart the system after the license expiration, the Premier features will not be loaded even if they are in the saved configuration. If you purchase a Premier license, you must obtain and install a license file. For more information about how to generate a license file, see *Getting Started with Avaya PLDS for Avaya Networking Products*, NN46199-300.

For more information about PLDS and installing a license file, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.

SFP+ transceivers

Release 4.1 introduces support for the following SFP+ transceivers.

Transceiver	Description	Part number
10GBASE-LR/LW (-5 °C to +85 °C)	1310 nm SMF with a range up to 10 km	AA1403011-E6HT
10GBASE-SR/SW (0 °C to +85 °C)	850 nm with a range up to 400 m (OM4)	AA1403015-E6HT

For more information, see *Installing Transceivers and Optical Components on Avaya Virtual Services Platform 8200,* NN47227-301.

SSL certificate management

This release adds support to manage an SSL certificate on the switch. You can install or remove a certificate, and configure the expiration time for a new certificate. This release also changes the default size of the certificate key length from 1,024 bits to 2,048 bits. The change in default size applies only to a new certificate; an existing certificate remains unchanged.

For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.

Simplified IGMP Access-Policy configuration

Release 4.1 supports simplified IGMP Access-Policy configuration, without having to specify VLAN IP subnet on the command line.

For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8200,* NN47227-504.

Overview of features and hardware models by release

This section provides an overview of the software features and hardware introduced in Releases 4.0.x and 4.1. For subsequent releases, the following table will expand to list new software features.

Note:

Each release includes all the features from previous releases unless specifically stated otherwise.

Features for Releases 4.0.x and 4.1

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

Features	New in this release				
	4.0	4.0.1	4.1		
Operations and Management					
Avaya CLI (ACLI) For more information, see *ACLI Commands Reference for Avaya Virtual Services Platform 8200,* NN47227-104.	X				
Configuration and Orchestration Manager (COM) For more information, see Avaya Configuration and Orchestration Manager (COM) documentation, http://support.avaya.com/.	X				
Domain Name Service (DNS) client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.	X				
Domain Name Service (DNS) client (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.			X		
Enterprise Device Manager (EDM) For more information, see *Using ACLI and EDM on Avaya Virtual Services Platform 8200,* NN47227-103.	X				
E-Tree and Private VLANs • For more information about E-Tree, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510. • For more information about private VLANs, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 8200,* NN47227-500 . • For information about configuring MultiLink Trunks (MLT) and Private VLANs, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8200,* NN47227-503.			X		
File Transfer Protocol (FTP) server/client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.	X				
File Transfer Protocol (FTP) server/client (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.			X		
Flight Recorder (for system health monitoring) For more information, see *Troubleshooting Avaya Virtual Services Platform 8200,* NN47227-700.	X				

Table continues…

Features	New in this release				
	4.0	4.0.1	4.1		
IEEE 802.1ag Connectivity Fault Management (CFM) • Layer 2 Ping • TraceRoute • TraceTree For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.	X				
802.1x-2001 Extended Authentication Protocol (EAP) and EAP over LAN (EAPoL)			X		
Key Health Indicator (KHI) For more information, see *Managing Faults on Avaya Virtual Services Platform 8200,* NN47227-702.	X				
Logging (log to file and syslog [IPv4]) For more information, see *Managing Faults on Avaya Virtual Services Platform 8200,* NN47227-702.	X				
Logging (log to file and syslog [IPv6]) For more information, see *Managing Faults on Avaya Virtual Services Platform 8200,* NN47227-702.			X		
Mirroring (port and flow-based) For more information, see *Troubleshooting Avaya Virtual Services Platform 8200,* NN47227-700.	X				
Network Time Protocol (NTP) For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.	X				
RADIUS, Community-based Users (IPv4) For more information, see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.	X				
RADIUS (IPv6) For more information, see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.			X		
Remote Login (Rlogin) server/client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.	X				
Remote Login (Rlogin) server (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.			X		

Table continues…

Features	New in this release				
	4.0	4.0.1	4.1		
Remote Shell (RSH) Server/Client For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.	X				
RMON For more information, see *Monitoring Performance on Avaya Virtual Services Platform 8200,* NN47227-701.	X				
Secure Copy (SCP) For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.	X				
Secure Shell (SSH) v1 and v2 server/client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.	X				
Secure Sockets Layer (SSL) certificate management For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.			X		
SSH server (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.			X		
SLA Mon™ For more information, see *Monitoring Performance on Avaya Virtual Services Platform 8200,* NN47227-701.			X		
Simple Loop Prevention Protocol (SLPP) For more information, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 8200,* NN47227-500.	X				
Simple Network Management Protocol (SNMP) v1/2/3 (IPv4) For more information, see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.	X				
SNMP (IPv6) For more information, see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.			X		
SoNMP (Avaya topology discovery protocol) For more information, see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.	X				
`spbm-config-mode` boot flag		X			

Table continues…

Features	New in this release				
	4.0	4.0.1	4.1		
For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8200,* NN47227-504.					
TACACS+ For more information, see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.			X		
Telnet server/client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.	X				
Telnet server/client (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.			X		
Trivial File Transfer Protocol (TFTP) server/client (IPv4) For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.	X				
Trivial File Transfer Protocol (TFTP) server/client (IPv6) For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.			X		
Virtual Link Aggregation Control Protocol (VLACP) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8200,* NN47227-503.	X				
Layer 2					
Avaya VENA Switch Cluster (Multi-Chassis LAG) • Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8200,* NN47227-503.	X				
Media Access Control Security (MACsec) For more information, see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.			X		
Microsoft Network Load Balancing Service (NLBS) • Unicast mode For more information, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 8200,* NN47227-500.	X				
MultiLink Trunking (MLT) / Link Aggregation Group (LAG)	X				

Table continues…

Features	New in this release				
	4.0	4.0.1	4.1		
For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8200,* NN47227-503.					
Spanning Tree Protocol (STP) • Multiple Spanning Tree Protocol (MSTP) • Rapid Spanning Tree Protocol (RSTP) For more information, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 8200,* NN47227-500.	X				
Avaya VENA Fabric Connect					
All Avaya Fabric Connect services with Switch Cluster For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.	X				
Equal Cost Trees (ECT) For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.	X				
Inter-VSN Routing For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.	X				
IPv6 Inter-VSN Routing For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.			X		
IP Multicast over SBPM For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.			X		
IP Shortcut Routing including ECMP For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.	X				
IPv6 Shortcut Routing For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.			X		

Table continues…

Features	New in this release				
	4.0	4.0.1	4.1		
IS-IS accept policies For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.			X		
Layer 2 Virtual Service Network (VSN) For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.	X				
Layer 3 VSN For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.			X		
`run spbm` installation script For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.			X		
Layer 3 IPv4 and IPv6 Routing Services					
Address Resolution Protocol (ARP) • Proxy ARP • Static ARP For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8200,* NN47227-505.	X				
Border Gateway Protocol (BGP) for IPv4 For more information, see *Configuring BGP Services on Avaya Virtual Services Platform 8200,* NN47227–508.			X		
Dynamic Host Configuration Protocol (DHCP) Relay, DHCP Option 82 For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8200,* NN47227-505.	X				
Equal Cost Multiple Path (ECMP) For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8200,* NN47227-505.	X				
Internet Control Message Protocol (ICMP) For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8200,* NN47227-505.	X				
Internet Group Management Protocol (IGMP) , including virtualization		X			

Table continues…

Features	New in this release				
	4.0	4.0.1	4.1		
For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8200,* NN47227-504.					
IP Route Policies For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8200,* NN47227-505.	X				
IPv6 (OSPFv3, VRRP, RSMLT, DHCP Relay, IPv4 in IPv6 tunnels) For more information, see *Configuring IPv6 Routing on Avaya Virtual Services Platform 8200,* NN47227–507.			X		
Layer 3 Switch Cluster (Routed SMLT) with Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on Avaya Virtual Services Platform 8200,* NN47227-503.	X				
Layer 3 Switch Cluster (Routed SMLT) with Simplified vIST For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8200,* NN47227-504.		X			
Open Shortest Path First (OSPF) For more information, see *Configuring OSPF and RIP on Avaya Virtual Services Platform 8200,* NN47227-506.	X				
Protocol Independent Multicast–Sparse Mode (PIM-SM), PIM-Source Specific Mode (PIM-SSM) For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8200,* NN47227-504.		X			
Route Information Protocol (RIP) For more information, see *Configuring OSPF and RIP on Avaya Virtual Services Platform 8200,* NN47227-506.	X				
Static Routing For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8200,* NN47227-505.	X				
Virtualization with IPv4 Virtual Routing and Forwarding (VRF) • ARP • DHCP Relay • Inter-VRF Routing (static, dynamic, and policy) • Local Routing	X				

Table continues…

Features	New in this release				
	4.0	4.0.1	4.1		
• OSPFv2 • RIPv1/2 • Route Policies • Static Routing • VRRP For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8200,* NN47227-505.					
Virtual Router Redundancy Protocol (VRRP) • Avaya Backup Master For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8200,* NN47227-505.	X				
Quality-of-Service and Filtering					
Access Control List (ACL)-based filtering • Egress ACLs • Ingress ACLs • Layer 2–Layer 4 Filtering • Port • VLAN For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8200,* NN47227-502.	X				
Access Control List (ACL)-based filtering • Egress ACLs • Ingress ACLs • Layer 2–Layer 4 Filtering • Port • VLAN For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8200,* NN47227-502.	X				
IPv6 ACL filters For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8200,* NN47227-502.			X		
Avaya Auto QoS	X				

Table continues…

Features	New in this release				
	4.0	4.0.1	4.1		
For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8200,* NN47227-502.					
Differentiated Services (DiffServ) including Per-Hop Behavior For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8200,* NN47227-502.	X				
Egress Port Shaper For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8200,* NN47227-502.	X				
Layer 2–Layer 4 Ingress Port Rate Limiter For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8200,* NN47227-502.	X				

VSP 8200 Series hardware models

The following table provides a listing of the hardware models introduced in the Virtual Services Platform 8200 Series.

Model	Part number	Release
VSP 8284XSQ-AC (AC power supply)	EC8200x01-E6 **Note:** Replace the “x” with a country-specific power cord code listed in Hardware compatibility on page 25.	4.0
VSP 8284XSQ-DC (DC power supply)	EC8200001-E6	4.0.50.0
VSP 8284XSQ AC PS No PC GSA (TAA-compliant; no power cord)	EC8200A01-E6GS	4.0.50.0
VSP 8284XSQ AC PS NA PC GSA (TAA-compliant; North American power cord)	EC8200E01-E6GS	4.0.50.0

For more information about hardware, see Hardware compatibility on page 25, and *Installing the Avaya Virtual Services Platform 8200,* NN47227-300.

VSP 4000 and VSP 8000 feature differences

Avaya has implemented feature parity between the VSP 4000 Series and the VSP 8000 Series in all but a few exceptions. Some features are supported in one platform and not the other to maintain compatibility with previous releases. In other cases, it has to do with the role of the switch in the network.

The following table summarizes the feature differences between the VSP 4000 and VSP 8000 in Release 4.1:

Feature	VSP 4000	VSP 8000
CMAC — CFM	Supported	Not Supported
COM	*	*
VMS Endura scripts	Supported	Not Supported
FDB protect by port	Supported	Not Supported
NLB Unicast	Not Supported	Supported
QoS	Supported	Supported with exceptions: • Classification does not have routed packet classification • No ingress policer- Uses ingress port rate limiting instead
Transparent UNI	Supported	Not Supported

* COM does not currently support the VSP 4000 or VSP 8000 for Release 4.1, but support is planned in a future COM release. The EDM plug-in (COM war file) is provided with Release 4.1 software so that it will be available to you when COM supports Release 4.1.

Other changes

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

Introduction chapter

The Introduction chapter has been updated to include information about searching a documentation collection.

Chapter 3: Important notices

This section describes the supported hardware and software scaling capabilities and provides important information for this release.

Hardware compatibility

The following tables describe the VSP 8284XSQ hardware.

Table 1: Hardware

VSP 8284XSQ	Description	Part number
VSP 8284XSQ-AC This model number ships with one field-replaceable 800 watt **AC** power supply.	• eighty 10 GbE SFP/SFP+ ports • four 40 GbE QSFP+ ports • one 10/100/1000 Base-T Out-Of-Band Management Port • one RJ-45 Console Port (10101) • one USB port • Base Software License • four field-replaceable fan trays	EC8200x01-E6 **Note:** Replace the “x” with a country-specific power cord code. See the footnote for details.
VSP 8284XSQ-DC This model number ships with one field-replaceable 800 watt **DC** power supply. **Note:** This model is supported in Release 4.1.1.	Includes all of the above features.	EC8200001-E6
VSP 8284XSQ AC PS No PC GSA This model number is compliant with the Trade Agreements Act (TAA). It ships with one field-	Includes all of the above features.	EC8200A01-E6GS

Table continues…

VSP 8284XSQ	Description	Part number
replaceable 800 watt **AC** power supply but no power cord.		
VSP 8284XSQ AC PS NA PC GSA This model number is also TAA compliant and ships with an **AC** power supply. However, it includes a North American power cord.	Includes all of the above features.	EC8200E01-E6GS
Redundant power supplies		
800 watt AC redundant power supply	The VSP 8284XSQ comes with one 800 W AC PSU. For full power redundancy, you can install a redundant 800 W AC PSU.	EC8005x01-E6 **Note:** Replace the “x” with a country-specific power cord code. See the footnote for details.
800 watt DC redundant power supply **Note:** This model is supported in Release 4.1.1.	The VSP 8284XSQ comes with one 800 W DC PSU. For full power redundancy, you can install a redundant 800 W DC PSU.	EC8005001-E6
*__Note__: The character (x) in the order number indicates the power cord code. Replace the “x” with the proper letter to indicate desired product nationalization. See the following for details: “A”: No power cord included. “B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden. “C”: Includes power cord commonly used in the United Kingdom and Ireland. “D”: Includes power cord commonly used in Japan. “E”: Includes North American power cord. “F”: Includes Australian power cord.		
Redundant fan trays		
12 volt redundant fan tray	The VSP 8284XSQ comes with all four 12–V fan trays installed.	EC8011004-E6
VSP 8000 Universal Slide Rack Mount Kit (300mm-900mm) **Note:** The slide rack mount kit is optional and must be ordered separately.		

Table continues…

VSP 8284XSQ	Description	Part number
300mm–900mm slide rack mount kit	The VSP 8284XSQ comes with a bracket to install the chassis on a tray. To install the chassis without a tray, install the slide rack mount kit.	EC8011002-E6

Compatible transceivers

Important:

Avaya recommends using Avaya-branded SFP, SFP+, and QSFP+ transceivers as they have been through extensive qualification and testing. Avaya will not be responsible for issues related to non-Avaya branded transceivers.

- The VSP 8000 operates in forgiving mode for SFP transceivers, which means that the switch will bring up the port operationally when using non-Avaya SFP transceivers. Avaya does not provide support for operational issues related to these SFPs, but they will operate and the port link will come up. The switch logs the device as an unsupported or unknown device.
- The VSP 8000 operates in strict mode for SFP+ and QSFP+ transceivers, which means that the switch will not bring the port up operationally when using non-Avaya SFP+ or QSFP+ transceivers.
- The VSP 8000 operates in forgiving mode for SFP+ and QSFP+ direct attached cables, which means that the switch will bring up the port operationally when using Non-Avaya direct attached cables. Avaya does not provide support for operational issues related to these DACs, but they will operate and the port link will come up.

For more information about compatible transceivers, see *Installing Transceivers and Optical Components on Avaya Virtual Services Platform 8200,* NN47227-301.

Software scaling capabilities

This section lists software scaling capabilities of the VSP 8284XSQ.

Table 2: Software scaling capabilities

	Maximum number supported
Layer 2	
MAC table size (Without SPBM)	224,000
MAC table size (With SPBM)	112,000
Port-based VLANs	4,059
Protocol-based VLAN (IPv6 only)	1
Multiple Spanning Tree Protocol (MSTP) instances	12
Rapid Spanning Tree Protocol (RSTP) instances	1

Table continues…

	Maximum number supported
LACP aggregators	84
Ports per LACP aggregator	16 (8-active, 8-standby)
MultiLink Trunking (MLT) groups	84
Ports per MLT group	8
SLPP VLANs	128
VLACP interfaces	84
Layer 3	
IPv4 VRF instances	24
IP Interfaces (IPv4/IPv6)	506
Routed Split Multi-Link Trunking (RSMLT) interfaces (IPv4 or IPv6)	252
VRRP interfaces (IPv4/IPv6)	252
VRRP interfaces with fast timers (200ms) - IPv4/IPv6	24
IPv4 Circuitless IP interfaces	256
IPv6 Circuitless IP interfaces	1
IPv4 Address Resolution Protocol (ARP) table	32,000
IPv6 neighbor table	8,000
IPv4 static ARP entries	2,000 for each VRF 10,000 for the switch
IPv6 static neighbor records	256
IPv4 route table size with "ipv6-mode" boot flag set to false	16,000
IPv6 route table size (Prefix Length < 64 bits) with "ipv6-mode" boot flag set to false	8,000
IPv6 route table size (Prefix Length > 64 bits) with "ipv6-mode" boot flag set to false	0
IPv4 route table size with "ipv6-mode" boot flag set to true	8,000
IPv6 route table size (Prefix Length < 64 bits) with "ipv6-mode" boot flag set to true	4,000
IPv6 route table size (Prefix Length > 64 bits) with "ipv6-mode" boot flag set to true	2,000
IPv6 6in4 configured tunnels	506
IPv4 static routes	1,000 per VRF 5,000 for the switch
IPv6 static routes	1,000
ECMP Groups/Paths per group	1,000/8

Table continues…

	Maximum number supported
IPv4 NLB interfaces	256
RIP interfaces	200
OSPF v2/v3 interfaces	500
OSPF v2/v3 neighbors (adjacencies)	500
OSPF areas	12 for each VRF 80 for each switch
e-BGP peers	12
IPv4 RIP routes	2,000 for each VRF 2,000 for the switch
IPv4 OSPF routes	16,000 for each VRF 16,000 for the switch **Note:** The maximum routes supported per VRF is 16,000. The 16,000 routes can be distributed across the 24 VRFs (+ GRT) in any manner.
IPv4 eBGP routes	16,000
IPv4 shortcut routes	16,000
IPv6 OSPFv3 routes - GRT only	8000
IPv6 shortcut routes – GRT only	8,000
IPv4 route policies	500 for each VRF 5,000 for the switch
IP Multicast	
IGMP interfaces	4,059
PIM interfaces	128 (Active), 256 (Passive)
PIM neighbors (GRT Only)	128
PIM-SSM static channels	4,000
Multicast receivers or IGMP Joins (per Switch)	6,000
Multicast senders (per Switch)	6000
Total multicast routes (per Switch)	6,000
Static multicast routes	4,000
Multicast enabled Layer 2 VSN	2,000
Multicast enabled Layer 3 VSN	24
SPBM	
SPBM enabled switches per region (BEB + BCB)	2,000
Service endpoint switches (BEBs) per I-SID	512

Table continues…

	Maximum number supported
IS-IS interfaces	84
IS-IS adjacencies	84
Layer 2 VSNs per switch (VLANs mapped to I-SID)	4,059
Layer 3 VSNs per switch (VRF mapped to I-SID)	24
E-Tree	
Number of private VLANs	4,059
Filters and QoS	
Total IPv4 Ingress rules (Port/VLAN based, Security/QoS filters)	766
Total IPv4 Egress rules (Port based, Security filters)	252
Total IPv6 Ingress rules (Port/VLAN based, Security/QoS filters)	256
Diagnostics	
Mirrored ports	83
OAM	
FTP sessions (IPv4/IPv6)	4 each
Rlogin sessions (IPv4/IPv6)	8 each
SSH sessions (IPv4/IPv6)	8 total (any combination of IPv4 and IPv6 up to 8)
Telnet sessions (IPv4/IPv6)	8 each, 16 total

File names for Release 4.1

This section describes the VSP 8284XSQ software files.

The following table provides the details of the software files. The file sizes are approximate.

Table 3: Software Build

Module or File Type	Description	File Name	File Size (in bytes)
Standard Runtime Software Image	Standard image for the VSP 8200 Series	VSP8200.4.1.0.0.tgz	46,866,824

Table 4: Software files

Description	File name	Size
Encryption modules	VSP8200.4.1.0.0_modules.tgz	41,831

Table continues…

Description	File name	Size
EDM Help File	VSP8200v410_HELP_EDM_gzip.zip	2,850,488
MIB Files	• VSP8200.4.1.0.0_mib.zip • VSP8200.4.1.0.0_mib.txt	• 812,196 • 5,256,142

Caution:

To download the software and files, use one of the following browsers: IE 9 or greater, or Mozilla Firefox. Do not use Google Chrome to download software and files.

Important:

After you download the software, calculate and verify the md5 checksum. To calculate and verify the md5 checksum on the device, see Calculating and verifying the md5 checksum for a file on a switch on page 31.To calculate and verify the md5 checksum on a Unix or Linux machine, see Calculating and verifying the md5 checksum for a file on a client workstation on page 32. On a Windows machine, use the appropriate Windows utility that is supported on your Windows version.

Calculating and verifying the md5 checksum for a file on a switch

Perform this procedure on a VSP switch to verify that the software files downloaded properly to the switch. Avaya provides the md5 checksum for each release on the Avaya Support website.

Before you begin

- Download the md5 checksum to an intermediate workstation or server where you can open and view the contents.
- Download the .tgz image file to the switch.

About this task

Calculate and verify the md5 checksum after you download software files.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Use the **ls** command to view a list of files with the `.tgz` extension:

   ```
   ls *.tgz
   ```

3. Calculate the md5 checksum for the file:

   ```
   md5 <filename.tgz>
   ```

4. Compare the number generated for the file on the switch with the number that appears in the md5 checksum on the workstation or server. Ensure that the md5 checksum of the software

suite matches the system output generated from calculating the md5 checksum from the downloaded file.

Example

The following example provides output for VSP 8200 but the same process can be used on other VSP switches.

View the contents of the md5 checksum on the workstation or server:

```
3242309ad6660ef09be1b945be15676d  VSP8200.4.1.0.0_edoc.tar
d000965876dee2387f1ca59cf081b9d6  VSP8200.4.1.0.0_mib.txt
897303242c30fd944d435a4517f1b3f5  VSP8200.4.1.0.0_mib.zip
2fbd5eab1c450d1f5feae865b9e02baf  VSP8200.4.1.0.0_modules.tgz
a9d6d18a979b233076d2d3de0e152fc5  VSP8200.4.1.0.0_OpenSource.zip
8ce39996a131de0b836db629b5362a8a  VSP8200.4.1.0.0_oss-notice.html
80bfe69d89c831543623aaad861f12aa  VSP8200.4.1.0.0.tgz
a63a1d911450ef2f034d3d55e576eca0  VSP8200v4.1.0.0.zip
62b457d69cedd44c21c395505dcf4a80  VSP8200v400_HELP_EDM_gzip.zip
```

Calculate the md5 checksum for the file on the switch:

```
Switch:1>ls *.tgz
-rw-r--r--  1 0       0         44015148 Dec  8 08:18  VSP8200.4.1.0.0.tgz
-rw-r--r--  1 0       0         44208471 Dec  8 08:19  VSP8200.4.1.0.0.tgz
Switch:1>md5 VSP8200.4.0.0.0.tgz
MD5 (VSP8200.4.1.0.0.tgz) = 80bfe69d89c831543623aaad861f12aa
```

Calculating and verifying the md5 checksum for a file on a client workstation

Perform this procedure on a Unix or Linux machine to verify that the software files downloaded properly. Avaya provides the md5 checksum for each release on the Avaya Support website.

About this task

Calculate and verify the md5 checksum after you download software files.

Procedure

1. Calculate the md5 checksum of the downloaded file:

   ```
   $ /usr/bin/md5sum <downloaded software-filename>
   ```

   Typically, downloaded software files are in the form of compressed Unix file archives (.tgz files).

2. Verify the md5 checksum of the software suite:

   ```
   $ more <md5-checksum output file>
   ```

3. Compare the output that appears on the screen. Ensure that the md5 checksum of the software suite matches the system output generated from calculating the md5 checksum from the downloaded file.

Example

The following example uses files from Avaya Virtual Services Platform 4000 Series but the same process applies to software files for all VSP switches.

Calculate the md5 checksum of the downloaded file:

```
$ /usr/bin/md5sum VSP4K.4.1.0.0.tgz

02c7ee0570a414becf8ebb928b398f51 VSP4K.4.1.0.0.tgz
```

View the md5 checksum of the software suite:

```
$ more VSP4K.4.1.0.0.md5
285620fdc1ce5ccd8e5d3460790c9fe1 VSP4000v4.1.0.0.zip

a04e7c7cef660bb412598574516c548f VSP4000v4100_HELP_EDM_gzip.zip
ac3d9cef0ac2e334cf94799ff0bdd13b VSP4K.4.1.0.0_edoc.tar
29fa2aa4b985b39843d980bb9d242110 VSP4K.4.1.0.0_mib_sup.txt
c5f84beaf2927d937fcbe9dd4d4c7795 VSP4K.4.1.0.0_mib.txt
ce460168411f21abf7ccd8722866574c VSP4K.4.1.0.0_mib.zip
1ed7d4cda8b6f0aaf2cc6d3588395e88 VSP4K.4.1.0.0_modules.tgz
1464f23c99298b80734f8e7fa32e65aa VSP4K.4.1.0.0_OpenSource.zip
945f84cb213f84a33920bf31c091c09f VSP4K.4.1.0.0_oss-notice.html
02c7ee0570a414becf8ebb928b398f51 VSP4K.4.1.0.0.tgz
```

Upgrading the software

Perform this procedure to upgrade the software on the VSP 8284XSQ. This procedure shows how to upgrade the software using the internal flash memory as the file storage location.

Before you begin

- Back up the configuration files.
- Transfer the upgrade file to the VSP 8284XSQ.

Important:

Avaya Virtual Services Platform 8200 software 4.0 is lenient in allowing mismatched autonegotiation settings between local ports and their remote link partners. VOSS 4.1 software requires same autonegotiation settings on link partners to avoid incorrect declaration of link status. Mismatched settings can cause the links to stay down. Ensure the autonegotiation settings between local ports and their remote link partners match before upgrading Avaya Virtual Services Platform 8200 software 4.0 to VOSS 4.1. For more information see, *Administering Avaya Virtual Services Platform 8200,* NN47227-600.

Note:

Software upgrade configurations are case sensitive.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Extract the release distribution files to the /intflash/release/ directory:

```
software add WORD<1-99>
```

3. Extract the module files to the /intflash/release directory:

```
Software add-module [software version] [modules file name]
```

4. Install the image:

```
software activate WORD<1-99>
```

5. Restart the switch:

```
reset
```

Important:

After you restart the switch, you have the amount of time configured for the commit timer to verify the upgrade and commit the software to gold. If you do not commit the software to gold and auto-commit is not enabled, the system restarts with the last known working version after the commit timer has expired. This feature ensures you can regain control of the system if an upgrade fails.

6. Confirm the software is upgraded:

```
show software
```

7. Commit the software:

```
software commit
```

Example

```
VSP-8284XSQ:1# software add VSP8200.4.1.0.0.tgz

VSP-8284XSQ:1# software add-modules 4.1.0.0.GA VSP8200.4.1.0.0_modules.tgz

VSP-8284XSQ:1# software activate 4.1.0.0.GA

VSP-8284XSQ:1# reset
```

```
VSP-8284XSQ:1#show software
================================================================================
                    software releases in /intflash/release/
================================================================================
VSP8200.4.1.0.0.GA (Primary Release)
    KERNEL                          2.6.32_int38
    ROOTFS                          2.6.32_int38
    APPFS                           VSP8K.4.1.0.0int031
  AVAILABLE ENCRYPTION MODULES
    No Modules Added


--------------------------------------------------------------------------------
Auto Commit     : enabled
Commit Timeout  : 10 minutes
```

```
VSP-8284XSQ:1# software commit
```

Shutting down the system

Use the following procedure to shut down the system.

Caution:

Before you unplug the AC power cord, always perform the following shutdown procedure. This procedure flushes any pending data to ensure data integrity.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Shut down the system:

   ```
   sys shutdown
   ```

3. Before you unplug the power cord, wait until you see the following message:

   ```
   System Halted, OK to turn off power
   ```

Example

Shut down a running system.

```
Switch:1#sys shutdown
Are you sure you want shutdown the system? Y/N  (y/n) ? y
CP1  [05/08/14 15:47:50.164] 0x00010813 00000000 GlobalRouter HW INFO System shutdown
initiated from CLI
CP1  [05/08/14 15:47:52.000] LifeCycle: INFO: Stopping all processes
CP1  [05/08/14 15:47:53.000] LifeCycle: INFO: All processes have stopped
CP1  [05/08/14 15:47:53.000] LifeCycle: INFO: All applications shutdown, starting power
down sequence
INIT: Sending processes the TERM signal
Stopping OpenBSD Secure Shell server: sshdno /usr/sbin/sshd found; none killed
Stopping vsp...Error, do this: mount -t proc none /proc
done
sed: /proc/mounts: No such file or directory
sed: /proc/mounts: No such file or directory
sed: /proc/mounts: No such file or directory
Deconfiguring network interfaces... done.
Stopping syslogd/klogd: no syslogd found; none killed
Sending all processes the TERM signal...
Sending all processes the KILL signal...
/etc/rc0.d/S25save-rtc.sh: line 5: /etc/timestamp: Read-only file system
Unmounting remote filesystems...
Stopping portmap daemon: portmap.
Deactivating swap...
Unmounting local filesystems...
[24481.722669] Power down.
[24481.751868] System Halted, OK to turn off power
```

Important information and restrictions

This section contains important information and restrictions you must consider before you use the VSP 8284XSQ.

Supported browsers

The VSP 8284XSQ supports the following browsers to access Enterprise Device Manager (EDM):

- Microsoft Internet Explorer 8.0
- Mozilla Firefox 32

User configurable SSL certificates

If you generate a certificate on the switch, you can configure only the expiration time.

If you need to configure other user parameters, you can generate a certificate off the switch and upload the key and certificate files to the `/intflash/ssh` directory. Rename the uploaded files to host.cert and host.key, and then reboot the system. The system loads the user-generated certificates during startup. If the system cannot find host.cert and host.key during startup, it generates a default certificate.

For more information about SSH and SSL certificates, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.

Interoperability notes for VSP 4000 or VSP 8000 connecting with ERS 5650

ERS 5650 operation causes a temporary loop that restarts the LACP-SMLT ports on the VSP 4000 or VSP 8000. This loop can shut down the LACP-SMLT port if SLPP is running on the port.

To prevent shutdown of the port on the switch, avoid using SLPP on LACP-SMLT ports.

Note:

When using Avaya ERS 5000 Series switches as SMLT edge devices with LACP-SMLT, use Advance LACP port mode on these switches to avoid the loop.

Chapter 4: Supported standards, RFCs, and MIBs

This chapter details the standards, request for comments (RFC), and Management Information Bases (MIB) that the VSP 8284XSQ supports.

Supported IEEE standards

The following table details the IEEE standards that the switch supports.

Table 5: Supported IEEE standards

IEEE standard	Description
802.1ag	Connectivity Fault Management
802.1ah	Provider Backbone Bridges (MacInMac encapsulation)
802.1aq	Shortest Path Bridging (SPB)
802.1ax	Link Aggregation Control Protocol (LACP)
802.1d	MAC bridges (Spanning Tree)
802.1p	VLAN prioritization
802.1q	Virtual Local Area Network (VLAN) tagging
802.1s	Multiple Spanning Tree Protocol
802.1t	802.1D maintenance
802.1w-2001	Rapid Spanning Tree Protocol (RSTP)
802.1x-2001	Extended Authentication Protocol (EAP) and EAP over LAN (EAPoL)
802.3 CSMA/CD Ethernet ISO/IEC 8802	International Organization for Standardization (ISO) / International Eletrotechnical Commission (IEC) 8802-3
802.3ab	Gigabit Ethernet 1000BaseT 4 pair Category 5 (Cat5) Unshieled Twisted Pair (UTP)
802.1ae	MACsec

Table continues…

IEEE standard	Description
802.3ae	10 Gigabit Ethernet
802.3x	flow control
802.3z	Gigabit Ethernet

Supported RFCs

The following table and sections list the RFCs that the switch supports.

Table 6: Supported request for comments

Request for comment	Description
draft-grant-tacacs-02.txt	TACACS+ Protocol
RFC768	UDP Protocol
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
RFC906	Bootstrap loading using TFTP
RFC950	Internet Standard Subnetting Procedure
RFC951	BootP
RFC959, RFC1350, and RFC2428	IPv6 FTP and TFTP client and server
RFC1027	Using ARP to implement transparent subnet gateways/Nortel Subnet-based VLAN
RFC1122	Requirements for Internet Hosts
RFC1155	Structure and Identification of Management Information for TCP/IP-based Internets
RFC1156	MIB for network management of TCP/IP
RFC1157	SNMP
RFC1212	Concise MIB definitions
RFC1215	Convention for defining traps for use with the SNMP
RFC1256	ICMP Router Discovery
RFC1258	BSD Rlogin server

Table continues…

Request for comment	Description
RFC1305	Network Time Protocol v3 Specification, Implementation and Analysis
RFC1340	Assigned Numbers
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)
RFC1493	Definitions of Managed Objects for Bridges
RFC1519	Classless Interdomain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC1542	Clarifications and Extensions for the Bootstrap Protocol
RFC1591	DNS Client
RFC1650	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC1724	RIPv2 MIB extensions
RFC1771	Border Gateway Protocol 4 (BGP-4)
RFC1772	Application of Border Gateway Protocol (BGP) in the internet
RFC1812	Router requirements
RFC1866	Hypertext Markup Language version 2 (HTMLv2) protocol
RFC1907	Management Information Base of the Simple Network Management Protocol version 2 (SNMPv2)
RFC1930	Guidelines for creation, selection, and registration of an Autonomous System (AS)
RFC1981	Path MTU Discovery
RFC1997	BGP Communities Attribute
RFC1998	Defining BGP communities
RFC2068	Hypertext Transfer Protocol
RFC2096	IP Forwarding Table MIB
RFC2131	Dynamic Host Control Protocol (DHCP)
RFC2138	RADIUS Authentication
RFC2139	RADIUS Accounting
RFC2233	Interfaces Group MIB using SMIv2
RFC2328	OSPFv2

Table continues…

Request for comment	Description
RFC2385	TCP MD5 Signature Option
RFC2439	BGP Route Flap Damping
RFC2454	Management Information Base for the User Datagram Protocol (UDP)
RFC2460	IPv6 Basic Specification
RFC2464	Transmission of IPv6 packets over Ethernet networks
RFC2474 and RFC2475	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC2578	Structure of Management Information Version 2 (SMIv2)
RFC2597	Assured Forwarding PHB Group
RFC2598	An Expedited Forwarding PHB
RFC2616	IPv6 Hypertext Transfer Protocol 1.1
RFC2674	Bridges with Traffic MIB
RFC2740	OSPF for IPv6
RFC2851	Textual Conventions for Internet Network Addresses
RFC2874	DNS Extensions for IPv6
RFC2932	IPv4 Multicast Routing MIB
RFC2933	IGMP MIB
RFC2934	PIM MIB
RFC2918	Route Refresh Capability for BGP-4
RFC2992	Analysis of an Equal-Cost Multipath Algorithm
RFC3046	DHCP Option 82
RFC3162	RADIUS and IPv6
RFC3315	DHCPv6 client/server/relay
RFC3411, RFC3412, RFC3413, RFC3414, and RFC3415	SNMP over IPv6 networks (SNMPv3)
RFC3416	v2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC3513	Internet Protocol Version 6 (IPv6) Addressing Architecture
RFC3587	IPv6 Global Unicast Address Format
RFC3596	DNS Extensions to Support IP Version 6
RFC3621	PoE – Power over Ethernet
RFC3768 and draft-ietf-vrrp-ipv6-spec-08.txt	IPv6 capable VRRP
RFC4007	IPv6 Scoped Address Architecture

Table continues…

Request for comment	Description
RFC4087	IP Tunnel MIB
RFC4213	IPv6 configured tunnel If support for tunneling and dual stack is required, the device must support Basic Transition Mechanisms for IPv6 Hosts and Routers
RFC4250, RFC4251, RFC4252, RFC4253, RFC4254, RFC4255, and RFC4256	SSH server and client support
RFC4291	IPv6 Addressing Architecture
RFC4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC4861	IPv6 Neighbor discovery
RFC4862	IPv6 stateless address autoconfiguration (SLAAC)
RFC5308	Routing IPv6 with IS-IS
RFC6329	IS-IS Extensions supporting Shortest Path Bridging

Standard MIBs

The following table details the standard MIBs that the switch supports.

Table 7: Supported MIBs

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
Link Aggregation Control Protocol (LACP) (802.3ad)	802.3ad	ieee802-lag.mib
SecY Management Table (secyIfTable)	802.1ae	ieee8021ae.mib
Exensible Authentication Protocol Over Local Area Networks (EAPoL) (802.1x)	802.1x	ieee8021x.mib
Internet Assigned Numbers Authority (IANA) Interface Type	—	iana_if_type.mib
MIB for network management of Transfer Control Protocol/Internet Protocol (TCP/IP)-based Internet MIB2	RFC1213	rfc1213.mib
A convention for defining traps for use with SNMP	RFC1215	rfc1215.mib

Table continues…

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
RIP Version 2 MIB Extension	RFC1389	rfc1389.mib
Definitions of Managed Objects for the Ethernet-like Interface Types	RFC1643	rfc1643.mib
BGP-4 MIB using SMIv2	RFC1657	rfc1657.mib
Remote Network Monitoring Management Information Base	RFC1757	rfc1757.mib
OSPF MIB	RFC1850	rfc1850.mib
IPv6 MIB: TCP MIB	RFC2452	rfc2452.mib
IPv6 MIB: UDP MIB	RFC2454	rfc2454.mib
IPv6 MIB: Textual Conventions and General Group MIB	RFC2465	rfc2465.mib
IPv6 MIB: ICMPv6 Group (ICMPv6) MIB	RFC2466	rfc2466.mib
Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework	RFC2576	rfc2576.mib
Definitions of Managed Objects for the Virtual Router Redundancy Protocol	RFC2787	rfc2787.mib
Textual Conventions for Internet Network Addresses	RFC2851	rfc2851.mib
The Interface Group MIB	RFC2863	rfc2863.mib
Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations	RFC2925	rfc2925.mib
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
Textual Conventions for IPv6 Flow Label	RFC3595	ipv6_flow_label.mib
Definitions of Managed Power over Ethernet	RFC3621	rfc3621.mib
The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model	RFC3826	rfc3826.mib

Table continues…

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
Management Information Base for the Transmission Control Protocol (TCP)	RFC4022	rfc4022.mib
IP Tunnel MIB	RFC4087	rfc4087.mib
Management Information Base for the User Datagram Protocol (UDP)	RFC4113	rfc4113.mib
Entity MIB	RFC4133	rfc4133.mib
Definitions of Managed Objects for Bridges	RFC4188	rfc4188.mib
Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions	RFC4363	p_bridge.mib and q_bridge.mib

Proprietary MIBs

The following table details the proprietary MIBs that the switch supports.

Table 8: Proprietary MIBs

Proprietary MIB name	File name
Avaya IGMP MIB	rfc_igmp.mib
Avaya IP Multicast MIB	ipmroute_rcc.mib
Avaya MIB definitions	wf_com.mib
Avaya PIM MIB	pim-rcc.mib
Avaya RSTP/MSTP proprietary MIBs	nnrst000.mib, nnmst000.mib
Avaya SLA Monitor Agent MIB	slamon.mib
Other SynOptics definitions	s5114roo.mib
Other SynOptics definitions	s5emt103.mib
Other SynOptics definitions	s5tcs112.mib
Other SynOptics definition for Combo Ports	s5ifx.mib
Other SynOptics definition for PoE	bayStackPethExt.mib
Rapid City MIB	rapid_city.mib

Table continues…

Proprietary MIB name	File name
Note: The MACsec tables, namely, rcMACSecCATable and rcMACSecIfConfigTable are a part of the Rapid City MIB.	
SynOptics Root MIB	synro.mib

Chapter 5: Known issues and limitations

This section details the known issues and limitations found in this release. Where appropriate, use the workarounds provided.

Table 9: Known issues and limitations

WI reference	Description
wi01174787	Using EDM, you cannot create static ARP entries. **Workaround:** Use the ACLI **`config ip arp`** command to create static ARP entries.
wi01195988	IPv4 Ping/TraceRoute may not work in the EDM. **Workaround:** Use ACLI to initiate ping and traceroute.
wi01196000	IPv6 Ping/TraceRoute may not work in the EDM. **Workaround:** Use ACLI to initiate ping and traceroute.
wi01197547	The output for the **`show vlan remote-mac-table`** command can be different than what appears for the same command on VSP 9000. Because all MinM packets that originate from the IST switch use the virtual B-MAC as the source BMAC, the remote BEB learns the C-MAC against the virtual B-MAC. Because the remote BEB uses the shortest path to the virtual B-MAC, the remote BEB can show the IST peer as a tunnel in the **`show vlan remote-mac-table`** command output.
wi01198259	IS-IS routes can stop being redistributed while configuring IS-IS Accept Policies. **Workaround:** Apply the accept policies again.
wi01203006	After creating an IPv4 filter to redirect next hop, the traffic does not get redirected to the new route even though the filter is hit and the next hop IP is reachable. **Workaround:** This issue occurs when the net hop IP is not reachable on rebooting the switch. Reconfigure the redirect next hop filter for ACLs once the route is up after reboot.
wi01203053	When there are two equal cost routes to a destination in different areas, increasing the cost of the learned interface more than the other interface has no effect on the route. **Workaround:** The issue is seen only when increasing the cost and only for inter-area routes. The issue is not seen when decreasing the cost. To see the effect on the route, disable and then enable OSPF after increasing the cost.

Table continues…

WI reference	Description
wi01204121	On using the command `show interface gigabitethernet statistics`, the OUTLOSS PACKETS counter value increments when packets are dropped as a result of Source Port squelching on NNI ports.
wi01204999	VSP devices as intermediate nodes, do not respond to the link trace request. VSP devices fail to respond to CFM link trace requests if the SPBm BVLANs are deleted and recreated with different BVLAN IDs. Issuing a node reboot after BVLAN ID change will restore Linktrace operation.
wi01205505	IPv6 ERCD and RCIP6 error logs are observed following IST reset. You may see the following errors when all RSMLT enabled VIST and UNI ports are shutdown: • REPLACE neighbor to HW FAILED • DELETE neighbor from HW FAILED • Failed to lookup Nexthop • Failed to update the stale bit for Neighbor The errors are logged intermittently when all NNI/VIST and UNI ports with RSMLT are shutdown or reset. These error logs occur due to the existence of a timing window during which RSMLT may try to clean-up VLAN when the port is already down. **Workaround:** Ignore these errors as there are no other ramifications and they do not cause any data loss.
wi01205572	Spoof-detect may not work when enabled. There are no commands to check the status of a spoof-detect port.
wi01205594	When CIST is disabled by admin, deleting an ISIS interface at port level may automatically enable CIST level mstp state.
wi01207076	If both IPv4 and IPv6 are configured on a vlan interface. Whenever IPv6 MTU is changed, IPv4 MTU also gets changes for that interface. **Workaround:** Set a higher MTU value upto 9500 bytes instead of the default MTU size of 1500 bytes that gets set when IPv6 is enabled on the vlan.
wi01207546	In configurations with at least three VRRP nodes with Back Master enabled on a non-SPB VLAN the VRRP state may continuously fluctuate between Master and Backup Master. Forwarding is not affected. **Workaround:** Only enable VRRP Backup Master if the node is running SPB and the VLAN is an SPB C-VLAN, for instance, an SMLT VLAN on a vIST node, otherwise do not enable VRRP Backup Master.
wi01207711	SPB ethertype 0x8100 is modfied to 0x88a8 when packets traverse over Virtual IST.
wi01208362	VSPtalk is referenced in "show fulltech". This has no impact on the switch operation.
wi01209346	In IGMP snoop environment, after dynamically downgrading the IGMP version to version 2 (v2), when you revert back to version 3 (v3), the following is observed: • the multicast traffic does not flow • the sender entries are not learned on the local sender switch

Table continues…

WI reference	Description
	• the Indiscard packet count gets incremented on the "show int gig error" statistics **Workaround:** Use a v3 interface as querier in a LAN segment which has snoop enabled v2 and v3 interfaces.
wi01209532	The port led on the device remains steady amber after removing the SFP+ pluggable from the port. This has no impact on the switch operation.
wi01209696	A corner case scenario where an IGMP ACL is applied to block a host from joining a particular group, while the Join record already exists for that host on the VSP, and if that host happens to be the only receiver on that interface, results in a node reboot. This happens only on IGMPv3 snoop enabled interface. **Workaround:** Use ACLs, even if you want to block the only receiver available on the interface.

Chapter 6: Resolved issues

This section details the issues that were resolved in this release.

Table 10: Resolved issues

WI reference	Description
wi01173503	If the configured number of IP interfaces exceeds the supported maximum, enabling IS-IS with IP shortcuts fails to take effect and the following error message is displayed. `Error: Insufficient resources available to create IP.` This issue was resolved in this release.
wi01176035	When you remove a fan, the switch incorrectly displays the wrong event ID and generates the following two messages: • `IO1 [06/13/14 14:52:18.541] 0x0011054c 00000000 GlobalRouter COP-SW INFO Master CP changed to slot 1` • `IO1 [06/13/14 14:53:27.541] 0x0011054c 00000000 GlobalRouter COP-SW INFO Master CP changed to slot 1` This issue was resolved in this release.
wi01176049	When you remove a fan, the switch incorrectly sends the following trap: `A rcnChasFanOk trap indicates that a fan unit of a fan tray in a fan zone has recovered from previously detected fan fault.` This issue was resolved in this release.
wi01194288	During an RSMLT failover, the 10 Gb link that is in process from DOWN state to UP state prematurely transmits the UP signal to the remote peer. This causes the remote side to switch the traffic to the VSP 8200 too early and causes a traffic loss of about 10-15 seconds. This issue was resolved in this release.
wi01195554	When the VSP 8200 is rebooting, the vIST is not established immediately. During this time, Layer 3 VSN traffic hashed to that VSP 8000 will be dropped. Typically, this traffic loss is for approximately 10 seconds. This issue was resolved in this release.