Release Notes for Avaya Virtual Services Platform 8284XSQ

Release 4.0.1
NN47227-401
Issue 02.05
December 2014

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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.

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.

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.

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 expected behaviors that may first appear to be issues.

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

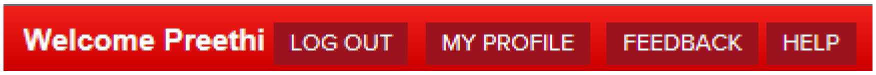
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

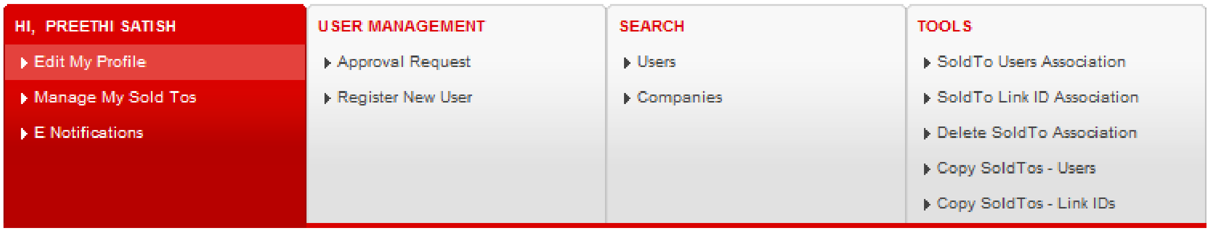
You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Ethernet Routing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

Procedure

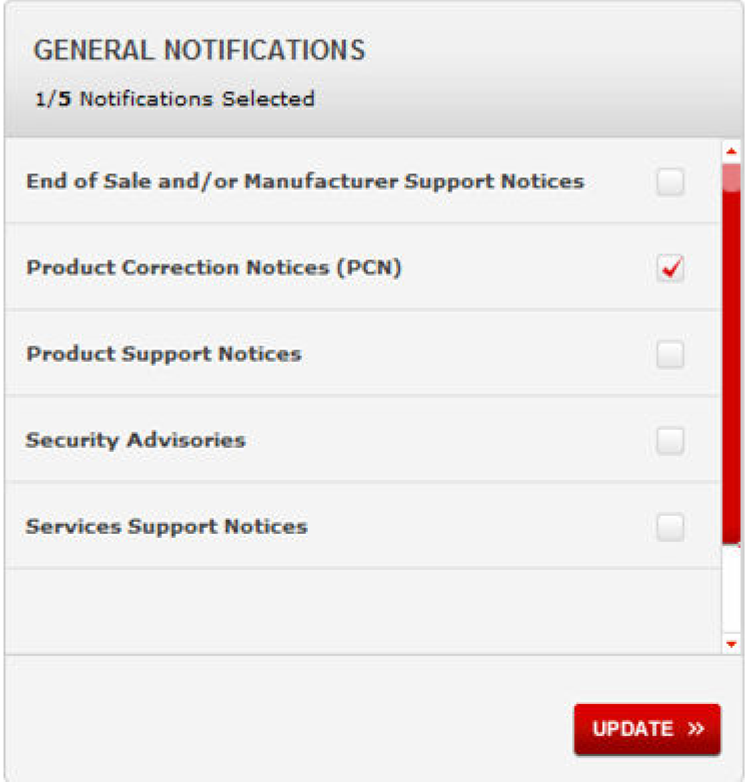
1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Click **MY PROFILE**.



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**.

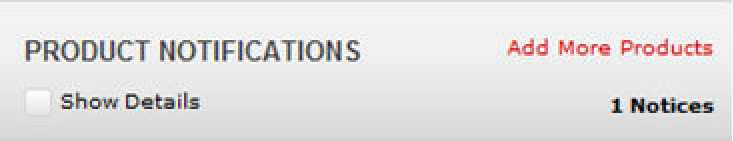


GENERAL NOTIFICATIONS

1/5 Notifications Selected

- End of Sale and/or Manufacturer Support Notices □
- Product Correction Notices (PCN) ☑
- Product Support Notices □
- Security Advisories □
- Services Support Notices □

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

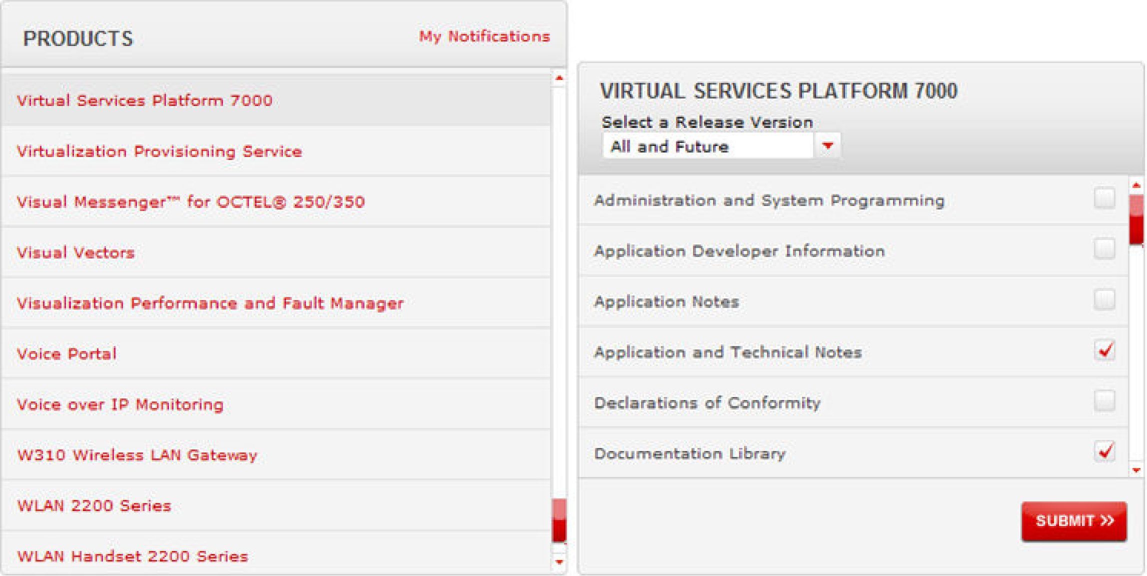


PRODUCT NOTIFICATIONS

□ Show Details

1 Notices

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.



PRODUCTS

My Notifications

- Virtual Services Platform 7000
- Virtualization Provisioning Service
- Visual Messenger™ for OCTEL® 250/350
- Visual Vectors
- Visualization Performance and Fault Manager
- Voice Portal
- Voice over IP Monitoring
- W310 Wireless LAN Gateway
- WLAN 2200 Series
- WLAN Handset 2200 Series

VIRTUAL SERVICES PLATFORM 7000

Select a Release Version: All and Future

- □ Administration and System Programming
- □ Application Developer Information
- □ Application Notes
- ☑ Application and Technical Notes
- □ Declarations of Conformity
- ☑ Documentation Library

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.

Chapter 2: New in this release

New in this release

The following sections detail what is new in *Release Notes for Avaya Virtual Services Platform 8200,* NN47227-401 for Release 4.0.1.

Overview of features and hardware models by release

This section provides an overview of the VSP 8284XSQ software features and hardware introduced in Releases 4.0.1. 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 4.0.1

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

Features	New in release			
	4.0	**4.0.1**		
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 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			

Features	New in release			
	4.0	4.0.1		
File Transfer Protocol (FTP) Server/Client 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			
IEEE 802.1ag Connectivity Fault Management (CFM) • L2 Ping • TraceRoute • TraceTree For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.	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) 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 For more information, see *Configuring Security on Avaya Virtual Services Platform 8200,* NN47227-601.	X			
Remote Login (Rlogin) Server/Client For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.	X			
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)	X			

Features	New in release			
	4.0	4.0.1		
For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.				
Secure Shell (SSH) v1 and v2 Server/Client For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.	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 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 For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8200,* NN47227-504.		X		
Telnet Server/Client For more information, see *Administering Avaya Virtual Services Platform 8200,* NN47227-600.	X			
Trivial File Transfer Protocol (TFTP) Server/Client 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			
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			

Features	New in release			
	4.0	4.0.1		
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				
Customer VLAN UNI with Avaya VENA 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			
IP Shortcut Routing including ECMP For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.	X			
L2 Virtual Service Network (VSN) For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 8200,* NN47227-510.	X			
Layer 3 IPv4 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			
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)	X			

Features	New in release			
	4.0	4.0.1		
For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8200,* NN47227-505.				
Internet Group Management Protocol (IGMP) For more information, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 8200,* NN47227-504.		X		
IP Route Policies For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 8200,* NN47227-505.	X			
L3 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			
L3 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 • OSPFv2 • RIPv1/2 • Route Policies • Static Routing	X			

Features	New in release			
	4.0	4.0.1		
• 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 • L2–L4 Filtering • Port • VLAN For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8200,* NN47227-502.	X			
Avaya Auto QoS For more information, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 8200,* NN47227-502.	X			
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			
L2–L4 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	EC8200x01-E6	4.0

Model	Part number	Release
	Note: Replace the “x” with a country-specific power cord code listed in Hardware compatibility on page 17.	

For more information about hardware, see Hardware compatibility on page 17, and *Installing the Avaya Virtual Services Platform 8200,* NN47227-300.

spbm-config-mode boot flag

Shortest Path Bridging (SPB) and Protocol Independent Multicast (PIM) cannot interoperate with each other on the switch at the same time. To ensure that SPB and PIM stay mutually exclusive, Avaya implemented a new boot flag called **`spbm-config-mode`**.

- The **`spbm-config-mode`** boot flag is enabled by default. This enables you to configure SPB and IS-IS, but you cannot configure PIM and IGMP either globally or on an interface.
- If you disable the boot flag, you can configure PIM and IGMP Snooping, but you cannot configure SPB or IS-IS.

Important:

- Any change to the **`spbm-config-mode`** boot flag requires a reboot for the change to take effect.
- If you plan to disable the boot flag, Avaya recommends that you remove all SPB configurations first.
- If you plan to use the default (enabled) setting, Avaya recommends that you remove all PIM configurations first.

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

Simplified Virtual-IST

Avaya introduced Simplified Virtual-IST (vIST) for non-SPB customers who are used to using SMLT with IST. The Simplified vIST feature provides a seamless migration of IST-based SMLT configurations to vIST-based SMLT configurations.

- Simplified vIST is available ONLY for non-SPB deployments when the boot flag (**`spbm-config-mode`**) is disabled.
- When the boot flag is enabled (default setting), Simplified vIST is not available so you configure SPB/ISIS for vIST as described in the Link Aggregation document.

Note:

You do not have to configure Simplified vIST in order to run PIM or IGMP Snooping in a non-SMLT topology.

Note:

- Virtual IST is not supported on LACP-enabled MLTs.
- You do not have to configure Simplified vIST in order to run PIM or IGMP Snooping in a non-SMLT topology.

After you disable the **`spbm-config-mode`** boot flag, you can configure PIM or IGMP Snooping on any VLAN including the vIST VLAN. You must configure PIM on the vIST VLAN if you expect that there will be local senders and receivers (non-SMLT) on the vIST peers whose route to the peer is via the V-IST VLAN.

Note:

Virtual IST is not supported on LACP-enabled MLTs.

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

IGMP versions

The Avaya Virtual Services Platform 8200 supports IGMPv1, IGMPv2, and IGMPv3. IGMPv2 and IGMPv3 are backward compatible and can exist together on a multicast network.

Protocol Independent Multicast-Sparse Mode

PIM-SM, as defined in RFC2362, supports multicast groups spread out across large areas of a company or the Internet. PIM-SM sends multicast traffic only to routers that specifically join a multicast group. This technique reduces traffic flow over WAN links and overhead costs for processing unwanted multicast packets.

Protocol Independent Multicast-Source Specific Multicast

Source Specific Multicast optimizes PIM-SM by simplifying the many-to-many model. Because most multicast applications distribute content to a group in one direction, SSM uses a one-to-many model that uses only a subset of the PIM-SM features. This model is more efficient and reduces the load on multicast routing devices.

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	• 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 • one USB port • Base Software License • one field-replaceable 800 Watt power supply • four field-replaceable fan trays	EC8200x01-E6 **Note:** Replace the “x” with a country-specific power cord code. See the footnote for details.
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.
*__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.		

VSP 8284XSQ	Description	Part number
"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.		
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

Table 2: Compatible 1000BASE SFPs

Hardware	Description	Minimum software version	Part number
Important: Avaya supports the SFPs with the following part numbers: AA1419013-E5, AA1419014-E5, AA1419015-E5, and AA1419025-E5 to AA1419040-E5. However, Avaya strongly recommends using the newer DDI versions of these SFPs.			
1000BASE-SX SFP	850 nm LC connector	4.0.0	AA1419013-E5
1000BASE-SX SFP	850 nm MT-RJ connector	4.0.0	AA1419014-E5
1000BASE-LX SFP	1310 nm LC connector	4.0.0	AA1419015-E5
1000BASE-XD CWDM SFP	From 1470 nm to 1610 nm LC connector, up to 40 km	4.0.0	AA1419025-E5 to AA1419032- E5
1000BASE-ZX CWDM SFP	From 1470 nm to 1610 nm LC connector, up to 70 km	4.0.0	AA1419033-E5 to AA1419040- E5
1000BASE-T (RJ-45) SFP	Gigabit Ethernet, RJ-45 connector	4.0.0	AA1419043-E6
1000BASE-SX (LC) DDI SFP	850 nm, Gigabit Ethernet, duplex LC connector	4.0.0	AA1419048-E6
1000BASE-LX (LC) DDI SFP	1310 nm, Gigabit Ethernet, duplex LC connector	4.0.0	AA1419049-E6
1000BASE-XD DDI SFP	1310 nm, Gigabit Ethernet, duplex LC connector	4.0.0	AA1419050-E6

Hardware	Description	Minimum software version	Part number
1000BASE-XD DDI SFP	1550 nm, Gigabit Ethernet, duplex LC connector	4.0.0	AA1419051-E6
1000BASE-ZX DDI SFP	1550 nm, Gigabit Ethernet, duplex LC connector	4.0.0	AA1419052-E6
1000BASE-XD CWDM (LC)	1470 nm to 1610 nm, up to 40 km	4.0.0	AA1419053-E6 to AA1419060–E6
1000BASE-ZX CWDM (LC)	1470 nm to 1610 nm, up to 70 km	4.0.0	AA1419061-E6 to AA1419068-E6
1000BASE-BX bidirectional SFP	1310 nm, single fiber LC, up to 10 km **Note:** Must pair with AA1419070-E6.	4.0.0	AA1419069-E6
1000BASE-BX bidirectional SFP	1490 nm, single fiber LC, up to 10 km **Note:** Must pair with AA1419069-E6.	4.0.0	AA1419070-E6
1000BASE-EX DDI SFP	1550 nm, up to 120 km	4.0.0	AA1419071-E6
1000BASE-BX bidirectional SFP	1310 nm, single fiber LC, up to 40 km **Note:** Must pair with AA1419077-E6.	4.0.0	AA1419076–E6
1000BASE-BX bidirectional SFP	1490 nm, single fiber LC, up to 40 km **Note:** Must pair with AA1419076-E6.	4.0.0	AA1419077–E6

Table 3: Compatible 10 Gigabit SFP+s

Hardware	Description	Minimum software version	Part number
10GBASE-LR/LW SFP+	1310 nm SMF with a range up to 10 km	4.0.0	AA1403011-E6
10GBASE-ER/EW SFP+	1550 nm SMF with a range up to 40 km	4.0.0	AA1403013-E6
10GBASE-SR/SW SFP+	850 nm with a range up to 300 m	4.0.0	AA1403015-E6
10GBASE ZR/ZW SFP+	1550 nm SMF with a range up to 70km	4.0.0	AA1403016-E6
10GBASE-LRM SFP+	220 m, 1260 to 1355 nm; 1310 nm nominal MMF	4.0.0	AA1403017-E6

Hardware	Description	Minimum software version	Part number
10GBase-CX	4-pair twinaxial copper cable that plugs into the SFP+ socket and connects two 10 Gb ports. The maximum range is 10m.	4.0.0	AA1403018-E6
10GBase-CX	4-pair twinaxial copper cable that plugs into the SFP+ socket and connects two 10 Gb ports. The maximum range is 3m.	4.0.0	AA1403019-E6
10GBase-CX	4-pair twinaxial copper cable that plugs into the SFP+ socket and connects two 10 Gb ports. The maximum range is 5m.	4.0.0	AA1403020-E6
10GBASE-ER CWDM DDI	1470 to 1610 nm with a range up to 40 km	4.0.0	AA1403153-E6 to AA1403160-E6
10GBASE-ZR CWDM DDI	1470 to 1610 nm with a range up to 70 km	4.0.0	AA1403161-E6 to AA1403168-E6

Table 4: Compatible 40 Gigabit QSFP+s transceivers

Hardware	Description	Minimum software version	Part number
QSFP+ to QSFP+ DAC	40G, 1 meter Passive DAC	4.0.0	AA1404029-E6
QSFP+ to QSFP+ DAC	40G, 3 meter Passive DAC	4.0.0	AA1404031-E6
QSFP+ to QSFP+ DAC	40G, 5 meter Passive DAC	4.0.0	AA1404032-E6
40GBase-LR4	40G QSFP+ (LC)	4.0.0	AA1404001-E6
40GBASE-SR4 / 4x10GBASE-SR	150m, MPO/MTP Connector	4.0.0	AA1404005-E6

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 5: Software scaling capabilities

	Maximum number supported
Layer 2	
IEEE/Port-based VLANs	4,059
LACP	84 aggregators
LACP ports per aggregator	8 active and 8 standby
MACs in forwarding database (FDB)	224,000
Multi-Link Trunking (MLT)	84 groups
Routed Split Multi-Link Trunking (RSMLT) IPv4 interfaces	252
Multiple Spanning Tree Protocol (MSTP)	64 instances
Protocol-based VLANs	1 (IPv6 only)
Rapid Spanning Tree Protocol (RSTP)	1 instance
SLPP	128 VLANs
VLACP Interfaces	84
Layer 3	
Address Resolution Protocol (ARP) for each port, VRF, or VLAN	32,000 entries total
Circuitless IP interfaces	64
ECMP groups	1000
ECMP paths per group	8
FIB IPv4 routes	16,000
IGMP interfaces	4059
IPv4 interfaces	506
NLB IPv4 interfaces (unicast support only)	256
IP routing policies	500 for each VRF 5,000 for the switch

	Maximum number supported
IPv4 FTP sessions	4
IPv4 Rlogin sessions	8
IPv4 SSH sessions	8
IPv4 Telnet sessions	8
IPv4 VRF instances	24
IPv4 Multicast source and group (S, G)	6,000 for each system, including VRFs
IPv4 Multicast static groups	4,000
IPv4 Multicast mroutes	12,000
IPv4 Multicast static source groups	4,000
Multicast IGMP instances	on 24 VRFs
OSPF interfaces	500
OSPF neighbors	500
OSPF areas	12 per VRF, 80 per switch
OSPF routes per VRF	16,000 16,000 **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.
OSPF routes	16,000
OSPF VRF support	24
PIM instances	on GRT only
PIM interfaces — active	128
PIM interfaces — passive	500
PIM neighbors	128
PIM-SSM static channels	4,000
RIP interfaces	200
RIP routes	16,000
Static ARP entries	2,000 for each VRF 10,000 for the switch
Static routes (IPv4)	1,000 per VRF 5,000 for the switch
UDP/DHCP forwarding entries	256 for each VRF 512 for the switch
VRRP interfaces (per VRF/per system)	64/128
VRRP interfaces fast timers (200 ms)	24

	Maximum number supported
Diagnostics	
Mirrored ports	83
Filters and QoS	
Port shapers (IPv4)	84
Access control lists (ACL) for each chassis	Ingress ACLs (inPort or inVlan): 256 • 256 ACLs with 1 security ACE each or • 128 ACLs with 1 QoS ACE each or • a combination based on this rule: ((num ACLs + num security ACEs) <= 512) && ((num ACLs + num QoS ACEs) <= 256) • This max implies a VLAN member count of 1 for inVlan ACLs. Egress ACLs (outPort only): 126 • 126 ACLs with 1 security ACE each (one of these ACLs can have 2 ACEs). • This max implies a port member count of 1 for outPort ACLs.
Access control entries (ACE) for each chassis (IPv4)	Ingress ACEs: 766 (Theoretical max of 766 implies 1 ingress ACL with 511 security ACEs & 255 QoS ACEs) • Ingress ACEs supported: (512(security) - # of ACLs) + (256(QoS) - # of ACLs). • This max also implies a VLAN member count of 1 for an inVlan ACL. Egress ACEs: 252 (Theoretical max of 252 implies 1 egress ACL with 252 security ACEs) • Egress ACEs supported: 253 - # of ACLs • This max also implies a port member count of 1 for the outPort ACL.
ACEs per ACL	766 on Ingress ACLs and 252 on Egress (all QoS, all security, or QoS and security combined).
Unique redirect next hop values for ACE Actions (IPv4)	Ingress: 1,018, Egress: 252
SPBM	
C-VLANs per VSP 8200 node	4,059
Maximum number of nodes per region	500

	Maximum number supported
MAC entries	112,000 (combination of ARP entries and Layer 2 MACs)
Backbone MAC	500
IP routes in the Global Router	10,000 for each VRF 16,000 for the switch
IS-IS interfaces	64
IS-IS adjacencies per VSP 8200 node	64
Layer 2 VSN ISIDs per VSP 8200 node	4,059

File names for this release

This section describes the VSP 8284XSQ software files.

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

Table 6: Software Build

Module or File Type	Description	File Name	File Size (in bytes)
Standard Runtime Software Image	Standard image for the VSP 8200 Series	VSP8200.4.0.1.0.tgz	44,208,471

Table 7: Software files

Description	File name	Size
Encryption modules	VSP8200.4.0.1.0_modules.tgz	41,831
EDM Help File	VSP8200v401_HELP_EDM_gzip.zip	2,275,488
MIB Files	• VSP8200.4.0.1.0_mib.zip • VSP8200.4.0.1.0_mib.txt	• 798,496 • 5,163,355

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.
- Ftp the upgrade file to the VSP 8284XSQ.

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 VSP8200.4.0.1.0.tgz

VSP-8284XSQ:1# software add-modules 4.0.1.0.GA VSP8200.4.0.1.0_modules.tgz

VSP-8284XSQ:1# software activate 4.0.1.0.GA

VSP-8284XSQ:1# reset
```

```
VSP-8284XSQ:1#show software
================================================================================
                    software releases in /intflash/release/
================================================================================
4.0.1.0GA (Primary Release)
VSP8200.4.0.1.0int025 (Backup Release)
VSP8200.4.0.1.0int022
VSP8200.4.0.1.0int020
--------------------------------------------------------------------------------
```

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

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

Shutting down the VSP 8200

Use the following procedure to shut down the VSP 8200.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Shut down the VSP 8200:

   ```
   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.

```
VSP8K-I Top: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

VSP 8284XSQ does not generate SSL certificates with user-configurable parameters. You can, however, use your own certificate.

You can generate a certificate off the VSP 8284XSQ 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.

SFP and SFP+ ports

SFP+ ports support 1G and 10G transceivers only.

For a complete list of supported SFPs and QSFPs, see Hardware compatibility on page 17.

vIST VLAN IP addresses

Do not configure a Rendezvous Point (RP) or Bootstrap Router (BSR) on the vIST VLAN because you cannot ping them outside of the vIST VLAN subnet. When you enter the **`ip pim enable`** command on the vIST VLAN, the following message displays:

```
WARNING: Please do not use virtual IST VLAN IP address for BSR and RP
related configurations, as unicast packets to virtual IST vlan IP address
from outside of  virtual IST vlan subnet will be dropped. Use Loopback or
CLIP interface IP address for BSR and RP related configurations.
```

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 VSP 8284XSQ supports.

Table 8: 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-2004	Port Based Network Access Control
802.3 CSMA/CD Ethernet ISO/IEC 8802	International Organization for Standardization (ISO) / International Eletrotechnical Commission (IEC) 8802-3
802.3ab	Gigabit Ethernet 1000BaseT 4 pair Category 5 (Cat5) Unshieled Twisted Pair (UTP)
802.3ae	10 Gigabit Ethernet
802.3x	flow control
802.3z	Gigabit Ethernet

Supported RFCs

The following table and sections list the RFCs that the VSP 8284XSQ supports.

Table 9: Supported request for comments

Request for comment	Description
RFC768	UDP Protocol
RFC783	Trivial File Transfer Protocol (TFTP)
RFC791	Internet Protocol (IP)
RFC792	Internet Control Message Protocol (ICMP)
RFC793	Transmission Control Protocol (TCP)
RFC826	Address Resolution Protocol (ARP)
RFC854	Telnet protocol
RFC894	A standard for the Transmission of IP Datagrams over Ethernet Networks
RFC896	Congestion control in IP/TCP internetworks
RFC906	Bootstrap loading using TFTP
RFC950	Internet Standard Subnetting Procedure
RFC951	BootP
RFC959, RFC1350, and RFC2428	FTP and TFTP client and server
RFC1027	Using ARP to implement transparent subnet gateways/Nortel Subnet based VLAN
RFC 1058	RIPv1 Protocol
RFC 1112	Host Extensions for IP Multicasting (IGMPv1)
RFC1122	Requirements for Internet Hosts
RFC 1253	OSPF
RFC1256	ICMP Router Discovery
RFC1305	Network Time Protocol v3 Specification, Implementation and Analysis
RFC1340	Assigned Numbers
RFC1519	Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC1541	Dynamic Host Configuration Protocol
RFC1542	Clarifications and Extensions for the Bootstrap Protocol
RFC 1583	OSPFv2
RFC 1587	The OSPF NSSA Option
RFC1591	DNS Client
RFC 1723	RIP v2 — Carrying Additional Information

Request for comment	Description
RFC1812	Router requirements
RFC1866	HyperText Markup Language version 2 (HTMLv2) protocol
RFC2068	Hypertext Transfer Protocol
RFC2131	Dynamic Host Control Protocol (DHCP)
RFC2138	RADIUS Authentication
RFC2139	RADIUS Accounting
RFC 2178	OSPF MD5 cryptographic authentication / OSPFv2
RFC 2236	IGMPv2 Snooping
RFC 2328	OSPFv2
RFC2338	VRRP: Virtual Redundancy Router Protocol
RFC 2362	PIM-SM
RFC 2453	RIPv2 Protocol
RFC2616	Hypertext Transfer Protocol 1.1
RFC 2740	OSPFv3
RFC2819	RMON
RFC2992	Analysis of an Equal-Cost Multi-Path Algorithm
RFC3046	DHCP Option 82
RFC 3376	IGMPv3
RFC 3569	An overview of Source-Specific Multicast (SSM)
RFC4250–RFC4256	SSH server and client support
RFC6329	IS-IS Extensions supporting Shortest Path Bridging

Quality of service

Table 10: Supported request for comments

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

Network management

Table 11: Supported request for comments

Request for comment	Description
RFC1155	SMI
RFC1157	SNMP
RFC1215	Convention for defining traps for use with the SNMP
RFC1271	Remote Network Monitoring Management Information Base
RFC1305	Network Time Protocol v3 Specification, Implementation and Analysis3
RFC1350	The TFTP Protocol (Revision 2)
RFC1354	IP Forwarding Table MIB
RFC1757	Remote Network Monitoring Management Information Base
RFC1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1908	Coexistence between v1 & v2 of the Internet-standard Network Management Framework
RFC1930	Guidelines for creation, selection, and registration of an Autonomous System (AS)
RFC2541	Secure Shell Protocol Architecture
RFC2571	An Architecture for Describing SNMP Management Frameworks
RFC2572	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC2573	SNMP Applications
RFC2574	User-based Security Model (USM) for v3 of the Simple Network Management Protocol (SNMPv3)
RFC2575	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC2576	Coexistence between v1, v2, & v3 of the Internet standard Network Management Framework
RFC2819	Remote Network Monitoring Management Information Base

MIBs

Table 12: Supported request for comments

Request for comment	Description
RFC1156	MIB for network management of TCP/IP
RFC1212	Concise MIB definitions
RFC1213	TCP/IP Management Information Base
RFC1354	IP Forwarding Table MIB
RFC1398	Ethernet MIB
RFC1442	Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1450	Management Information Base for v2 of the Simple Network Management Protocol (SNMPv2)
RFC1573	Interface MIB
RFC1650	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC2021	RMON MIB using SMIv2
RFC2096	IP Forwarding Table MIB
RFC2578	Structure of Management Information v2 (SMIv2)
RFC2674	Bridges with Traffic MIB
RFC2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC2863	Interface Group MIB
RFC2925	Remote Ping, Traceroute & Lookup Operations MIB
RFC3416	v2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC4113	Management Information Base for the User Datagram Protocol (UDP)

Standard MIBs

The following table details the standard MIBs that the VSP 8284XSQ supports.

Table 13: 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
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
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
STDMIB15—Remote Network Monitoring (RMON)	RFC2819	rfc2819.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

Standard MIB name	Institute of Electrical and Electronics Engineers/Request for Comments (IEEE/RFC)	File name
STDMIB26e—View-based Access Control Model (VACM) for the SNMP	RFC2575	rfc2575.mib
STDMIB26f —Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework	RFC2576	rfc2576.mib
STDMIB29—Definitions of Managed Objects for the Virtual Router Redundancy Protocol	RFC2787	rfc2787.mib
STDMIB31—Textual Conventions for Internet Network Addresses	RFC2851	rfc2851.mib
STDMIB32—The Interface Group MIB	RFC2863	rfc2863.mib
STDMIB33—Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations	RFC2925	rfc2925.mib
STDMIB35—Internet Group Management Protocol MIB	RFC2933	rfc2933.mib
STDMIB36—Protocol Independent Multicast MIB for IPv4	RFC2934	rfc2934.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

Proprietary MIBs

The following table details the proprietary MIBs that the VSP 8284XSQ supports.

Table 14: 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
PROMIB11 – Avaya MIB definitions	wf_com.mib
PROMIB12 – Other SynOptic definition for Combo Ports	s5ifx.mib
PROMIB31 – Other SynOptic definition for PoE	bayStackPethExt.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 15: Known issues and limitations

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.` **Workaround:** Delete the IP interfaces that are in excess of the supported scaling number and disable/enable IS-IS. Please note that this procedure will cause a disruption of services while IS-IS is being disabled and enabled again.
wi01174787	Using EDM, you cannot create static ARP entries. **Workaround:** Use the ACLI **`config ip arp`** command to create static ARP entries.
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` **Workaround:** None. This issue has no impact on the switch and can be ignored.
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.` **Workaround:** None. This issue has no impact on the switch and can be ignored.

Chapter 6: Resolved issues

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

Table 16: Resolved issues

WI reference	Description
wi01172005	Convergence times for traffic following link/switch failures within a SPB network are typically sub-second. However, there is a scenario where the convergence time exceeded the sub-second threshold when all but one of the NNI paths between a pair of Virtual IST peers go down simultaneously and the one remaining path between the Virtual IST peers is not a direct link. In this scenario, the Virtual IST could go down and come back up within a few seconds. A maximum traffic loss of up to 4 seconds was observed for a few flows when this happens. **This issue was resolved in this release.**
wi01174515	If you disable VRRP on a VLAN on an SMLT node in Backup Master state, there is a possibility of traffic loss on that VLAN lasting for up to 8 minutes. This issue only affects traffic that uses the VRRP VR as the gateway. **This issue was resolved in this release.**