Release Notes for VSP Operating System Software

Release 5.0
NN47227-401
Issue 07.02
February 2016

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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” 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.

“Hosted Service” means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” 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 is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage

Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or 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.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

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: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: https://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: https://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

Contents

Chapter 1: Introduction

Purpose

This document provides information on features in VSP Operating System Software (VOSS). VOSS runs on the following product families:

- Avaya Virtual Services Platform 4000 Series
- Avaya Virtual Services Platform 7200 Series
- Avaya Virtual Services Platform 8000 Series

This document describes important information about this release for the VOSS products.

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

For installation and initial setup information of the Open Networking Adapter (ONA), refer to the Quick Install Guide that came with your ONA.

Note:

The ONA works only with the Avaya Virtual Services Platform 4000 Series. For more information about configuring features, refer to the VOSS documentation. See *Documentation Reference for VSP Operating System Software*, NN47227-100 for a list of all the VSP 4000 documents.

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.

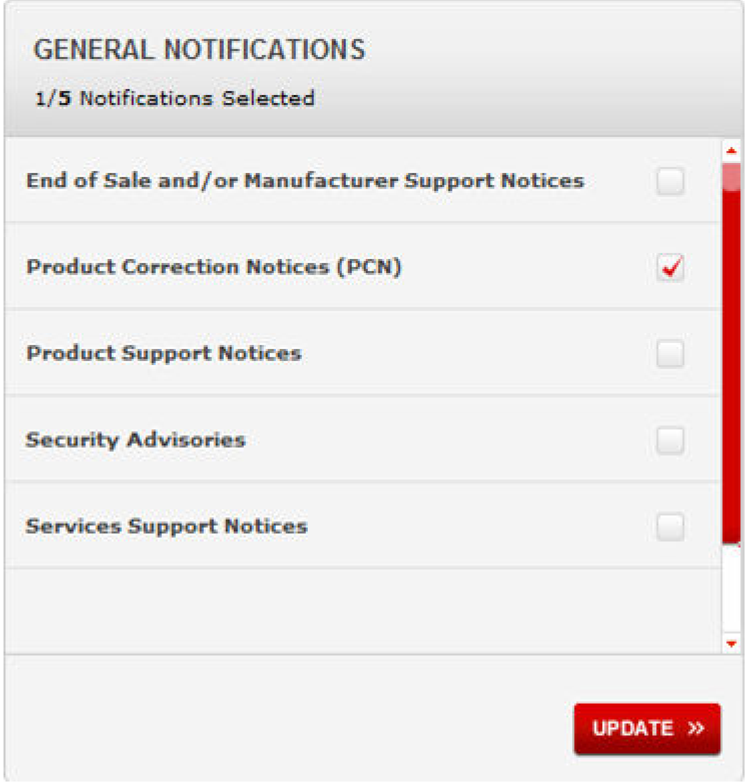
About this task

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 Virtual Services Platform 7000.

Procedure

1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.

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

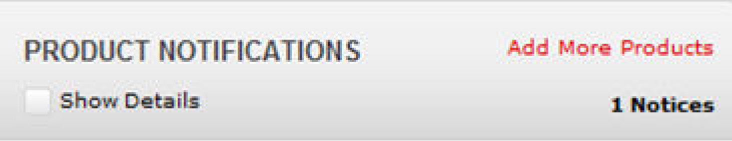


GENERAL NOTIFICATIONS

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**.

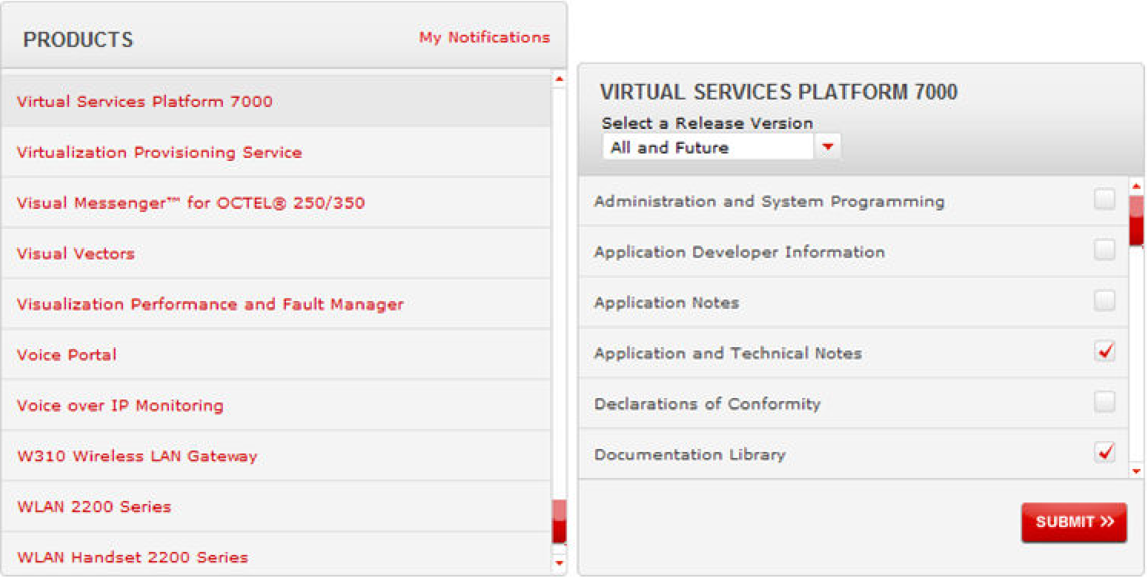


PRODUCT NOTIFICATIONS

□ 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 ☑
SUBMIT »

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 VSP Operating System Software*, NN47227-401.

New hardware

VOSS 5.0 supports the following new hardware:

- VSP 4000 Series
    - VSP 4450GSX-DC is a variant of Avaya Virtual Services Platform 4000 Series that ships with DC power supplies. It was introduced in Release 4.0.50.0, but not supported in Release 4.1, 4.2, or 4.2.1. It is now fully supported in Release 5.0. For more information, see *Installing Avaya Virtual Services Platform 4450GSX-PWR+ Switch*, NN46251-307.
- VSP 8404

    Ethernet Switch Modules (ESMs) provide physical interfaces on the VSP 8400. VOSS 5.0 release introduces three new ESMs:

    - 8418XTQ - 16 port 10GBASE-T and 2 port 40GBASE-QSFP+ Combination Ethernet Switch Module
    - 8424GS - 24 port 100/1000BASE-X Ethernet Switch Module
    - 8424GT - 24 port 10/100/1000BASE-T Ethernet Switch Module

    For more information, see *Installing the Avaya Virtual Services Platform 8000 Series*, NN47227-300
- Open Networking Adapter 1101GT

    Open Networking Adapter (ONA) 1101GT is a ruggedized, standalone device running a vSwitch platform on a hardened and tamper-proof Linux OS implementation. Though the ONA does not run VOSS 5.0, it is used with VSP 4000 Series to deliver Fabric Extend and Fabric Extend with fragmentation and reassembly functionality. The ONA 1101GT runs its own OS.

    For more information, see *Release Notes for Open Networking Adapter 1101GT*, NN48800-400.

Features

See the following sections for information about feature changes.

Fabric

VOSS 5.0 introduces the following Fabric enhancements.

Fabric Extend:

Key solution attributes of Avaya Fabric Connect have included rapid time to service, Layer 2 and Layer 3 Unicast and IP Multicast virtualization, fast network convergence in case of failures, and scalable IP multicast. Until now Fabric Connect required dedicated physical or emulated point-to-point Ethernet links to enable all fabric benefits. With the introduction of Avaya Fabric Extend, the Fabric Connect Core can now be extended across Broadcast Ethernet (referred to as FE-VID) and IP routed (referred to as FE-IP) networks..

This feature enables the extension of Fabric Connect to address the following customer needs:

- Data center interconnect (DCI) over IP WAN or Ethernet LAN services.
- Fabric overlay across a Layer 3 VPN service over an MPLS network.
- Fabric to the branch over IP MPLS VPNs, MPLS VPLS, or VLAN tunnels (Pseudo wire-MPLS or PBB E-Lines).
- Fabric Overlay for IP campus network

Important:

Some of the use cases above may require fragmentation and reassembly due to IP MTU limitations. For those situations, an ONA with VSP 4000 Series is required at both ends of the Fabric Extend connection to deliver Fabric Extend with fragmentation and reassembly.

For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.

Flex UNI — Switched UNI:

VOSS 5.0 introduces a new type of Flex-UNI, called Switched UNI. The Switched UNI type helps you manually create an I-SID and map many VLAN IDs and port or MLT lists to that I-SID. The I-SIDs thus created are ELAN I-SIDs.

I-SID is IEEE next generation VLAN. SPB supports 16 million unique services where as the VLAN supports 4096. SPB I-SID is a true service ID and once it is provisioned at the edge, the network core automatically interconnects like I-SID endpoints to create a contiguous service.

Note:

- You cannot enable EAPoL on Switched UNI ports because EAPoL does not support tagging and Switched UNI requires that the ports be tagged.

For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.

The following table identifies existing show commands modified for Switched UNI.

Command	Addition or update
`show ipv6 neighbor`	The attribute `PHYS INTF` is modified to show cvid/port or cvid/mlt for a Switched UNI physical interface.
`show ip arp`	The attribute `PORT` is modified to show cvid/port or cvid/mlt for a Switched UNI interface.
`show i-sid mac-address-entry`	The attribute `INTERFACE` is modified to show cvid/port or cvid/mlt for a Switched UNI interface.
`show vlan mac-address-entry`	The attribute `INTERFACE` is modified to show cvid/port or cvid/mlt for a Switched UNI interface.
`show i-sid`	A new attribute `ORIGIN` is added to show whether the i-sid was configured, discovered, or management.
`show interface gigabiteternet`	The attribute `FLEX-UNI` is added to show if Flex-UNI is enabled on the port.
`show mlt`	The attribute `FLEX-UNI` is added to show if Flex-UNI is enabled on the MLT.

Fabric Attach:

One of the key benefits of the Avaya Fabric Connect, an enhanced implementation of Shortest Path Bridging (SPB) technology, is simplified operations through access-layer-only network provisioning. Fabric Connect delivers a “Zero-Touch-Core” that virtually eliminates the chance of core network misconfiguration. It allows simple and secure deployment for any type of network service without the need to make any configuration changes on intermediate or core nodes, even in environments where clients roam. But until now, these benefits were available only on Fabric Connect capable devices.

Avaya has developed “Fabric Attach” to extend these same benefits to network elements or hosts that are NOT SPB-capable. Avaya Fabric Attach (FA) extends Fabric Connect to deliver an “Autonomic Edge” capability that dramatically reduces the costs of adding or modifying new or existing services. Any FA-capable device, for example, a switch, server, access point, or IP Phone, can now be securely connected to the network, be authorized for a network service, and attach to the appropriate network service instance – all automatically and based on IT policy.

Fabric Attach can be deployed in two ways:

- In the access layer(s) of any network.
- In the access layer(s) of an Avaya Fabric Connect network.

Fabric Attach – the key elements

- FA Server — An SPB capable network device at the Fabric Connect edge running in the FA Server mode to support downstream FA Proxy and FA Client devices. FA Servers are always network switching nodes supporting this function.
- FA Client — A network-attached end device running the FA Agent in FA Client mode. FA Clients can be Avaya Ethernet Routing Switches, WLAN 9100 Access Points, IP Phones, Hypervisors supporting FA Client on Open vSwitch, or other third party devices planned for the future.
- FA Proxy — A network device running the FA Agent in FA Proxy mode. FA Proxy switches can also support client mode for directly attached users or end devices. FA Proxies are always

network switching nodes supporting downstream FA Client devices, while directly connecting to an upstream FA Server device.

- FA Standalone Proxy— A non-SPB network device running the FA Agent in FA Proxy mode supporting FA Client devices, but without the need for an upstream FA Server. This is used where Fabric Attach is running in a non-Fabric Connect network.
- FA Policy Server — Avaya Identity Engines server, which can be optionally used in an FA solution to authenticate end-user and end devices. Network services (VLAN only or VLAN plus SPB services) can be created in the Fabric Attach environment based on authorization of the end user or end device.

Important:

VOSS 5.0 introduces FA Server functionality in the access layer(s) of an Avaya Fabric Connect network. FA Server on VOSS switches does not support interoperability with FA Proxy devices operating in standalone mode.

- FA Server

  When a switch is enabled as an FA Server, it receives IEEE 802.1AB Logical Link Discovery Protocol (LLDP) messages from FA Client and FA Proxy devices requesting the creation of Switched UNI service identifiers (I-SIDs). One FA Server can receive requests and consequently attach to multiple FA Client or Proxy devices. Similarly, a single client or proxy device can connect to multiple switches in SMLT configuration acting as the FA Server. The I-SIDs thus created, are able to join a Shortest Path Bridging (SPB) network.

- FA and Switched UNI

  The FA Server automatically creates Switched UNI I-SIDs and endpoints for port and MLT interfaces on which the feature is enabled and mapping requests are received.

  Both manually configured Switched UNI and automatically created FA I-SIDs and endpoints can co-exist on the same switch.

Important:

The FA Server only responds to FA signaling messages from FA Proxy switches configured to use the SPB provisioning mode.

The following tables identify the minimum GA software releases required to build an FA solution.

Table 1: Extending Fabric using Static FA Proxy configuration (ISID/VLAN is manually configured on FA Proxy)

FA Server		FA Proxy	
Product	**Minimum release**	**Product**	**Minimum release**
VSP 4000 VSP 7200 VSP 8200 VSP 8400	5.0.0.0	ERS 5900	7.0.1
		ERS 5600	6.6.3
		ERS 4800	5.9.2
		ERS 4500	5.7.3

Table 2: Extending Fabric to FA Clients by using FA Proxy

FA Server		FA Proxy		FA Policy	FA Client	
Product	**Minimum release**	**Product**	**Minimum release**		**Product**	**Minimum release**
VSP 4000 VSP 7200 VSP 8200 VSP 8400	5.0.0.0	ERS 5900	7.0.1	IDE Release 9.1 **Note:** See Note below.	AP9100	7.2.5
		ERS 5600	6.6.3			
		ERS 4800	5.9.2			
		ERS 4500	5.7.3			
Note: Required for AP9100 FA Client. IDE sends FA ISID/VLAN assignment request by using FA Proxy to VOSS FA Server.						

For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.

IS-IS external metric:

The current release introduces a metric type to differentiate between IS-IS internal and external routes. You can use the metric type as a match condition for accept policies and route redistribution.

> **Important:**
>
> For important interoperability considerations, see Interoperability considerations for IS-IS external metric on page 66.
>
> For important upgrade information, see Pre-upgrade instructions for IS-IS metric type on page 73.

For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.

Transparent UNI name update:

The documentation now refers to the Transparent UNI feature as Transparent Port UNI.

For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.

IPv6

VOSS 5.1 introduces the following IPv6-specific enhancements.

First Hop Security:

First Hop Security improves local network security by employing following RIPE 554 requirements for Layer 2 switches:

- DHCPv6-guard — A Layer 2 device filters DHCPv6 messages intended for DHCPv6 clients according to a number of different criteria. DHCPv6–guard protects against rogue DHCPv6 servers.
- Router Advertisement (RA)-guard — Filters router advertisements based on a set of criteria and designates a router authorization proxy. RA-guard provides a complimentary solution to

Secure Neighbor Discovery (SEND) environments where SEND might not be suitable or fully supported by all devices involved.

For more information, see *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 or *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601.

BGP+:

The current release extends the BGPv4 protocol to support the exchange of IPv6 routes using BGPv4 peering. BGP+ is an extension of BGPv4 for IPv6.

The current support is not an implementation of BGPv6. Native BGPv6 peering uses the IPv6 Transport layer (TCPv6) for establishing the BGPv6 peering, route exchanges, and data traffic. Native BGPv6 peering is not supported.

For more information, see *Configuring BGP Services on VSP Operating System Software*, NN47227-508.

RIPng:

Routers use RIPng to exchange information to compute routes through an IPv6 based network. IPv6 provides the neighbor router information RIPng requires. A RIPng router has interfaces in several networks and the protocol relies primarily on the metric of each network to compute routes using the distance vector algorithm.

For more information, see *Configuring IPv6 Routing on VSP Operating System Software*, NN47227-507.

CLIP:

The current release enhances IPv6 CLIP support to include the following:

- Use an IPv6 CLIP interface as the source IP for management protocols.
- Redistribute IPv6 CLIP interfaces as local routes in OSPFv3, RIPng, IS-IS, and BGP+.

The number of IPv6 CLIP interfaces is also increased to 64.

For more information, see *Configuring IPv6 Routing on VSP Operating System Software*, NN47227-507.

OSPFv2 and OSPFv3 Graceful Restart

The OSPF Graceful Restart feature is an enhancement to allow an OSPF router to stay on the forwarding path during the restart of its software. This is called graceful restart mode. Another part of this feature is how OSPF routers help other OSPF routers stay on the forwarding path while they restart their software. This is called helper mode. The current release supports only helper mode for both OSPFv2 and OSPFv3 protocols.

For more information, see the following documents:

- *Configuring OSPF and RIP on Avaya Virtual Services Platform 4000 Series*, NN46251-506
- *Configuring OSPF and RIP on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-506
- *Configuring IPv6 Routing on VSP Operating System Software*, NN47227-507

OSPFv3 RFC 5340 updates

The IPv6 OSPF module is compliant with OSPFv3 specified in RFC 5340, and it supports the following:

- Deprecation of MOSPF for IPV6
- NSSA Specification
- Stub Area Unknown LSA Flooding Restriction Deprecated
- Link LSA Suppression
- LSA Options and Prefix Options Updates
- IPv6 Site-Local Addresses

For more information, see the following documents:

- *Configuring OSPF and RIP on Avaya Virtual Services Platform 4000 Series*, NN46251-506
- *Configuring OSPF and RIP on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-506
- *Configuring IPv6 Routing on VSP Operating System Software*, NN47227-507

Secure Copy

VOSS 5.0 reintroduces Secure Copy (SCP). You can use SCP to securely transfer computer files between a local host and a remote host or between two remote hosts.

For more information, see the following documents:

- *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601
- *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600
- *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601
- *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600

SSH server authentication mode

The current release adds the **`ssh keyboard-interactive-auth`** command to change the SSH server authentication mode. By default, the SSH server uses password authentication but you can change the authentication mode to keyboard-interactive. If you use the ASG feature, the SSH server must use keyboard-interactive authentication.

For more information, see *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 or *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600.

Unicast Reverse Path Forwarding for IPv4 and IPv6

The current release adds support for unicast reverse path forwarding checking for both IPv4 and IPv6. Use this feature to prevent packet forwarding for incoming packets that have incorrect or forged (spoofed) addresses.

For more information, see the following documents:

- *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601

- *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601

USB troubleshooting

The current release adds the **`dos-chkdsk /usb`** command for the VSP 4450 model switches to achieve parity with VSP 7200 Series and VSP 8000 Series.

For more information, see *Troubleshooting of Avaya Virtual Services Platform 4000 Series*, NN46251-700.

Changes to pre-existing features

VOSS 5.0 makes the following support changes to pre-existing features.

`exception dump` command:

This release makes the **`exception dump`** command obsolete.

ICMP Redirect:

The following ICMP Redirect commands are no longer supported, including their **`no`** and **`default`** variations:

- **`ip icmp redirect`** in both Global Configuration and VRF Router Configuration modes.
- **`ipv6 icmp redirect-msg`** in Global Configuration mode.

MACsec replay-protect:

Starting with VOSS 5.0 release, support for the replay-protect option within MACsec configuration has been removed, as this option sometimes causes a black hole for traffic under certain situations such as node reboots across emulated Ethernet links. If replay-protect was previously enabled, upon upgrade to VOSS 5.0, replay-protect will be disabled on all interfaces where it was previously enabled. The replay-protect option is no longer visible or configurable in VOSS 5.0.

Note:

Removal of replay-protect option does NOT affect the core MACsec functionality of encryption or confidentiality protection. Core MACsec functionality of strong 128 bit encryption and confidentiality protection continues to be fully supported in VOSS 5.0 release.

See Important upgrade consideration on page 73 before you upgrade to VOSS 5.0 if replay-protect has been previously configured.

Remote Monitoring (RMON):

RMON1 (or legacy RMON) is not supported in VOSS 5.0. However, RMON2 is still supported.

RMON1 is the original version of the protocol, which collects information for OSI Layer 1 and Layer 2 in Ethernet networks. RMON2 monitors network and application layer protocols on configured network hosts that you enable for monitoring.

Overview of features by release and platform

This section provides an overview of which release introduced feature support for a particular platform. Each new release for a platform includes all the features from previous releases unless specifically stated otherwise.

Note:

4.1 is the first VOSS release. Release numbers earlier than 4.1 are releases specific to the particular platform.

Feature introduction

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

Features	Release by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
Operations and management				
Avaya CLI (ACLI) For more information, see *Using ACLI and EDM on VSP Operating System Software*, NN47227-103.	3.0	4.2.1	4.0	4.2
Channelization of 40 Gbps ports For more information, see *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600.	N/A	4.2.1	4.2	4.2
Configuration and Orchestration Manager (COM) For more information, see Avaya Configuration and Orchestration Manager (COM) documentation, http://support.avaya.com/.	3.0	4.2.1	4.0	4.2
Domain Name Service (DNS) client (IPv4) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	3.0	4.2.1	4.0	4.2
DNS client (IPv6) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.1	4.2.1	4.1	4.2
The encryption modules file is included in the runtime software image file; it is not a separate file.	4.2	4.2.1	4.2	4.2

Table continues…

Features	Release by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
Enhanced Secure mode For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.2	4.2.1	4.2	4.2
Enterprise Device Manager (EDM) For more information, see *Using ACLI and EDM on VSP Operating System Software*, NN47227-103.	3.0	4.2.1	4.0	4.2
EDM representation of physical LED status For more information, see the following documents: • *Installing Avaya Virtual Services Platform 4850GTS Series*, NN46251-300 • *Installing Avaya Virtual Services Platform 4450GTX-HT-PWR+ Switch*, NN46251–304 • *Installing Avaya Virtual Services Platform 4450GSX-PWR+ Switch*, NN46251-307 • *Installing the Avaya Virtual Services Platform 7200 Series*, NN47228-302 • *Installing the Avaya Virtual Services Platform 8000 Series*, NN47227-300	3.0	4.2.1	4.2	4.2
File Transfer Protocol (FTP) server/client (IPv4) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	3.0	4.2.1	4.0	4.2
FTP server/client (IPv6) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.1	4.2.1	4.1	4.2
Flight Recorder (for system health monitoring)	3.0	4.2.1	4.0	4.2

Table continues…

Features	Release by platform series			
	VSP 4000	**VSP 7200**	**VSP 8200**	**VSP 8400**
For more information, see the following documents: • *Troubleshooting of Avaya Virtual Services Platform 4000 Series*, NN46251-700 • *Troubleshooting Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-700				
IEEE 802.1ag Connectivity Fault Management (CFM) • Layer 2 Ping • TraceRoute • TraceTree For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	3.1	4.2.1	4.0	4.2
Extensible Authentication Protocol (EAP) and EAP over LAN (EAPoL) For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.1	4.2.1	4.1	4.2
Key Health Indicator (KHI) For more information, see the following documents: • *Fault Management of Avaya Virtual Services Platform 4000 Series*, NN46251-702 • *Managing Faults on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-702	3.0	4.2.1	4.0	4.2
Logging (log to file and syslog [IPv4]) For more information, see the following documents: • *Fault Management of Avaya Virtual Services Platform 4000 Series*, NN46251-702 • *Managing Faults on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-702	3.0	4.2.1	4.0	4.2
Logging (log to file and syslog [IPv6]) For more information, see the following documents: • *Fault Management of Avaya Virtual Services Platform 4000 Series*, NN46251-702	4.1	4.2.1	4.1	4.2

Table continues…

Features	Release by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
• *Managing Faults on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-702				
Mirroring (port and flow-based) For more information, see the following documents: • *Troubleshooting of Avaya Virtual Services Platform 4000 Series*, NN46251-700 • *Troubleshooting Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-700	3.0	4.2.1	4.0	4.2
Network Time Protocol (NTP) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	3.0	4.2.1	4.0	4.2
Non EAPoL MAC RADIUS authentication For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.2.1	4.2.1	4.2.1	4.2.1
RADIUS, community-based users (IPv4) For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	3.0	4.2.1	4.0	4.2
RADIUS (IPv6) For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.1	4.2.1	4.1	4.2
Remote Login (Rlogin) server/client (IPv4)	3.0	4.2.1	4.0	4.2

Table continues…

Features	Release by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600				
Rlogin server (IPv6) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.1	4.2.1	4.1	4.2
Remote Monitoring 1 (RMON1) for Layer 1 and Layer 2 ✱ **Note:** RMON1 is not supported in VOSS 5.0 or later.	3.0	4.2.1	4.0	4.2
Remote Monitoring 2 (RMON2) for network and application layer protocols For more information, see the following documents: • *Performance Management of Avaya Virtual Services Platform 4000 Series*, NN46251-701 • *Monitoring Performance on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-701	4.2	4.2.1	4.2	4.2
Remote Shell (RSH) server/client For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	3.0	4.2.1	4.0	4.2
Russia summer time zone change For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.2	4.2.1	4.2	4.2
Secure Copy (SCP)	3.0	5.0	4.0	5.0

Table continues…

Features	Release by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
Note: Release 4.2 and 4.2.1 do not support SCP. For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600				
Secure FTP (SFTP) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	3.0	4.2.1	4.0	4.2
Secure hash algorithm 1 (SHA-1) and SHA-2 For more information, see the following documents: • *Configuring OSPF and RIP on Avaya Virtual Services Platform 4000 Series*, NN46251-506 • *Configuring OSPF and RIP on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-506	4.2	4.2.1	4.2	4.2
Secure Shell (SSH) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	3.0	4.2.1	4.0	4.2
Secure Sockets Layer (SSL) certificate management For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.1	4.2.1	4.1	4.2
SSH (IPv6) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600	4.1	4.2.1	4.1	4.2

Table continues…

Features	Release by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
• *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600				
SLA Mon™ For more information, see the following documents: • *Performance Management of Avaya Virtual Services Platform 4000 Series*, NN46251-701 • *Monitoring Performance on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-701	4.1	4.2.1	4.1	4.2
Simple Loop Prevention Protocol (SLPP) For more information, see the following documents: • *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 4000 Series*, NN46251-500 • *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-500	3.0	4.2.1	4.0	4.2
Simple Network Management Protocol (SNMP) v1/2/3 (IPv4) For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	3.0	4.2.1	4.0	4.2
SNMP (IPv6) For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.1	4.2.1	4.1	4.2
SoNMP (Avaya topology discovery protocol) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	3.0	4.2.1	4.0	4.2
`spbm-config-mode` boot flag	4.1	4.2.1	4.0.1	4.2

Table continues…

Features	Release by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
For more information, see the following documents: • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series* , NN46251-504 • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-504				
TACACS+ For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.0	4.2.1	4.1	4.2
Telnet server/client (IPv4) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	3.0	4.2.1	4.0	4.2
Telnet server/client (IPv6) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.1	4.2.1	4.1	4.2
Trivial File Transfer Protocol (TFTP) server/client (IPv4) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	3.0	4.2.1	4.0	4.2
TFTP server/client (IPv6) For more information, see the following documents: • *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 • *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600	4.1	4.2.1	4.1	4.2

Table continues…

Features	Release by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
Virtual Link Aggregation Control Protocol (VLACP) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on VSP Operating System Software*, NN47227-503.	3.0	4.2.1	4.0	4.2
Layer 2				
Avaya switch cluster (multi-chassis LAG) • Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on VSP Operating System Software*, NN47227-503.	4.1	4.2.1	4.0	4.2
First Hop Security For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	5.0	5.0	5.0	5.0
Media Access Control Security (MACsec) **Note:** VOSS 5.0 officially removes the replay protection commands. Do not use replay protection in earlier releases. For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.0	4.2.1	4.1	4.2
Microsoft Network Load Balancing Service (NLBS) • Unicast mode For more information, see *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-500.	N/A	4.2.1	4.0	4.2
MultiLink Trunking (MLT) / Link Aggregation Group (LAG) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on VSP Operating System Software*, NN47227-503.	3.0	4.2.1	4.0	4.2

Table continues…

Features	Release by platform series			
	VSP 4000	**VSP 7200**	**VSP 8200**	**VSP 8400**
Spanning Tree Protocol (STP) • Multiple Spanning Tree Protocol (MSTP) • Rapid Spanning Tree Protocol (RSTP) For more information, see the following documents: • *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 4000 Series*, NN46251-500 • *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-500	3.0	4.2.1	4.0	4.2
Avaya Fabric technologies				
All Fabric Connect services with Avaya switch cluster For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.1	4.2.1	4.0	4.2
Equal Cost Trees (ECT) For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	3.0	4.2.1	4.0	4.2
E-Tree and Private VLANs • For more information about E-Tree, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510. • For more information about Private VLANs, see the following documents: - *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 4000 Series*, NN46251-500 - *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-500 • For information about how to configure MultiLink Trunks (MLT) and Private VLANs, see *Configuring Link Aggregation, MLT, SMLT, and vIST on VSP Operating System Software*, NN47227-503.	3.0.1	4.2.1	4.1	4.2
Fabric Attach For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	5.0	5.0	5.0	5.0
Fabric Extend For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	5.0	5.0	5.0	5.0
Inter-VSN routing	3.0	4.2.1	4.0	4.2

Table continues…

Features	Release by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.				
IPv6 inter-VSN routing For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.1	4.2.1	4.1	4.2
IP Multicast over Fabric Connect For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	3.1	4.2.1	4.1	4.2
IP Shortcut routing including ECMP For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	3.0	4.2.1	4.0	4.2
IPv6 Shortcut routing For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.1	4.2.1	4.1	4.2
IS-IS accept policies For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.1	4.2.1	4.1	4.2
Layer 2 Virtual Service Network (VSN) For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	3.0	4.2.1	4.0	4.2
Layer 3 VSN For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	3.0	4.2.1	4.1	4.2
`run spbm` installation script For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.1	4.2.1	4.1	4.2
`run vms endura` script For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	4.1	N/A	N/A	N/A
Switched UNI For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	5.0	5.0	5.0	5.0
Transparent Port UNI (T-UNI) For more information, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.	3.1	4.2.1	4.2.1	4.2.1
Layer 3 IPv4 and IPv6 routing services				

Table continues…

Features	Release by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
Address Resolution Protocol (ARP) • Proxy ARP • Static ARP For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	3.0	4.2.1	4.0	4.2
Border Gateway Protocol (BGP) for IPv4 For more information, see *Configuring BGP Services on VSP Operating System Software*, NN47227-508.	3.1	4.2.1	4.1	4.2
BGP+ (BGP for IPv6) For more information, see *Configuring BGP Services on VSP Operating System Software*, NN47227-508.	5.0	5.0	5.0	5.0
Internal Border Gateway Protocol (IBGP) For more information, see *Configuring BGP Services on VSP Operating System Software*, NN47227-508.	4.2	4.2.1	4.2	4.2
External Border Gateway Protocol (EBGP) For more information, see *Configuring BGP Services on VSP Operating System Software*, NN47227-508.	3.1	4.2.1	4.1	4.2
Dynamic Host Configuration Protocol (DHCP) Relay, DHCP Option 82 For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	3.0	4.2.1	4.0	4.2
Equal Cost Multiple Path (ECMP) For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	3.0	4.2.1	4.0	4.2
Gratuitous ARP filtering	4.2	4.2.1	4.2	4.2

Table continues…

Features	Release by platform series			
	VSP 4000	**VSP 7200**	**VSP 8200**	**VSP 8400**
For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505				
Internet Control Message Protocol (ICMP) For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	3.0	4.2.1	4.0	4.2
Internet Group Management Protocol (IGMP) , including virtualization For more information, see the following documents: • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series* , NN46251-504 • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-504	3.0	4.2.1	4.0.1	4.2
IP route policies For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	3.0	4.2.1	4.0	4.2
IPsec for IPv6 For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	4.2	4.2.1	4.2	4.2
IPv6 (OSPFv3, VRRP, RSMLT, DHCP Relay, IPv4 in IPv6 tunnels) For more information, see *Configuring IPv6 Routing on VSP Operating System Software*, NN47227-507.	4.1	4.2.1	4.1	4.2
Layer 3 switch cluster (Routed SMLT) with Virtual Inter-Switch Trunk (vIST)	4.1	4.2.1	4.0	4.2

Table continues…

Features	Release by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on VSP Operating System Software*, NN47227-503.				
Layer 3 switch cluster (Routed SMLT) with Simplified vIST For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST on VSP Operating System Software*, NN47227-503.	4.1	4.2.1	4.0.1	4.2
Open Shortest Path First (OSPF) For more information, see the following documents: • *Configuring OSPF and RIP on Avaya Virtual Services Platform 4000 Series*, NN46251-506 • *Configuring OSPF and RIP on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-506	3.1	4.2.1	4.0	4.2
Protocol Independent Multicast–Sparse Mode (PIM-SM), PIM-Source Specific Mode (PIM-SSM) For more information, see the following documents: • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 4000 Series* , NN46251-504 • *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-504	4.1	4.2.1	4.0.1	4.2
Route Information Protocol (RIP) For more information, see the following documents: • *Configuring OSPF and RIP on Avaya Virtual Services Platform 4000 Series*, NN46251-506 • *Configuring OSPF and RIP on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-506	3.1	4.2.1	4.0	4.2
RIPng For more information, see *Configuring IPv6 Routing on VSP Operating System Software*, NN47227-507.	5.0	5.0	5.0	5.0
Static routing For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	3.0	4.2.1	4.0	4.2

Table continues…

Features	Release by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
Unicast Reverse Path Forwarding (URPF) checking (IPv4 and IPv6) For more information, see the following documents: • *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601 • *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601	5.0	5.0	5.0	5.0
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 • VRRP For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	3.0	4.2.1	4.0	4.2
Virtual Router Redundancy Protocol (VRRP) • Avaya Backup Master For more information, see the following documents: • *Configuration - IP Routing for Avaya Virtual Services Platform 4000 Series*, NN46251-505 • *Configuring IP Routing on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-505	3.0	4.2.1	4.0	4.2
Quality of Service and filtering				
Access Control List (ACL)-based filtering • Egress ACLs • Ingress ACLs • Layer 2 to Layer 4 filtering	3.0	4.2.1	4.0	4.2

Table continues…

Features	Release by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
• Port • VLAN For more information, see the following documents: • *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series*, NN46251-502 • *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-502				
Avaya Auto QoS For more information, see the following documents: • *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series*, NN46251-502 • *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-502	3.0	4.2.1	4.0	4.2
Differentiated Services (DiffServ) including Per-Hop Behavior For more information, see the following documents: • *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series*, NN46251-502 • *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-502	3.0	4.2.1	4.0	4.2
Egress port shaper For more information, see the following documents: • *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series*, NN46251-502 • *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-502	3.0	4.2.1	4.0	4.2
IPv6 ACL filters For more information, see the following documents: • *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series*, NN46251-502 • *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-502	4.1	4.2.1	4.1	4.2

Table continues…

Features	Release by platform series			
	VSP 4000	VSP 7200	VSP 8200	VSP 8400
Layer 2 to Layer 4 ingress port rate limiter For more information, see the following documents: • *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series*, NN46251-502 • *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-502	3.0	4.2.1	4.0	4.2

VOSS feature differences

Avaya has implemented feature parity between the VSP Operating System Software (VOSS) platforms in all but a few exceptions. Some features are supported in one platform and not another to maintain compatibility with previous releases. In other cases, the difference is because of the role of the switch in the network.

The following table summarizes the feature differences between the platforms in this release.

Feature	VSP 4000 Series	VSP 7200 Series	VSP 8000 Series
Channelization of 40 Gbps ports	Not applicable	Supported	Supported
CMAC — CFM	Supported	Not supported	Not supported
Endura scripts	Supported	Not supported	Not supported
FDB protected by port	Supported	Not supported	Not supported
NLB unicast	Not supported	Supported	Supported
QoS	Supported	Supported with exceptions: • Classification does not have routed packet classification • No ingress policer-Uses ingress port rate limiting instead	Supported with exceptions: • Classification does not have routed packet classification • No ingress policer-Uses ingress port rate limiting instead
Software licensing (Premier)	Supports the Avaya Data Licensing Portal and the Product Licensing & Delivery System (PLDS)	Supports Product Licensing & Delivery System (PLDS) only	Supports Product Licensing & Delivery System (PLDS) only
Use of Open Networking Adapter for Fabric Extend	Required	Not required	Not required

Note:

COM support for VSP 7200 Series and VSP 8400 is planned for COM Release 3.1.2.

Chapter 3: Important notices

This section describes the supported hardware and software scaling capabilities, and provides important information for this release. Unless specifically stated otherwise, the notices in this section apply to all VOSS platforms.

Hardware compatibility

This section lists the hardware compatibility for all VOSS platforms.

Hardware compatibility for VSP 4000 Series

This section lists the Avaya Virtual Services Platform 4000 Series hardware and indicates the software release support.

Note:

4.1 is the first VOSS release. Release numbers earlier than 4.1 are releases specific to VSP 4000.

Part numbers that end in GS are the TAA-compliant version of the hardware.

VSP 4000 hardware

Part number	Model number	Initial release	Supported release					
			4.0.40	4.0.50	4.1	4.2	4.2.1	5.0
EC4400004-E6	VSP 4450GSX-DC	4.0.50	—	Y	—	—	—	Y
EC4400A03-E6	VSP 4450GTX-HT-PWR+ (no power cord)	4.0.40	Y	—	Y	Y	Y	Y
EC4400E03-E6	VSP 4450GTX-HT-PWR+ (NA power cord)	4.0.40	Y	—	Y	Y	Y	Y
EC4400x05-E6 Note: Replace the “x” with a country specific power cord	VSP 4450GSX-PWR+	4.0	—	—	Y	Y	Y	Y

Table continues…

Part number	Model number	Initial release	Supported release					
			4.0.40	4.0.50	4.1	4.2	4.2.1	5.0
code. See the footnote for details.								
EC4400A05-E6GS	VSP 4450GSX-PWR+ TAA Compliant (no power cord)	4.0.50	—	Y	—	—	Y	Y
EC4400E05-E6GS	VSP 4450GSX-PWR+ TAA Compliant (NA power cord)	4.0.50	—	Y	—	—	Y	Y
EC4800078-E6	VSP 4850GTS DC	3.0	—	—	Y	Y	Y	Y
EC4800x78-E6 EC4800x78-E6GS Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 4850GTS	3.0	—	—	Y	Y	Y	Y
EC4800x88-E6 EC4800x88-E6GS Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 4850GTS-PWR+	3.0	—	—	Y	Y	Y	Y
Note: The character (x) in the order number indicates the power cord code. Replace the “x” with the proper letter to indicate the 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.								

Compatible transceivers

Important:

Avaya recommends using Avaya-branded SFP, and SFP+ 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 4000 Series 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 4000 Series operates in strict mode for SFP+ transceivers, which means that the switch will not bring the port up operationally when using non-Avaya SFP+ transceivers.
- The VSP 4000 Series operates in forgiving mode for SFP+ 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 VSP Operating System Software*, NN47227-301.

Important operational note for VSP 4000 switches

This section provides information to take into consideration to prevent system operation failure.

Operational consideration for USB Flash Drive on factory supplied and converted VSP 4000 switches
Warning: The USB FLASH drive on all models of VSP 4850 (factory built and converted from ERS 4850) must be treated as a permanent non-removable part of the switch and must NEVER be removed from the switch to ensure proper operation. Additionally, the USB cover must be installed to ensure additional protection against removal. The USB FLASH drive on the VSP 4850 switch is uniquely and permanently bound to the operating system of the switch it is first used on and cannot be transferred to a different switch. Removal (and reinsertion) of the USB FLASH drive from the switch is not supported as it can permanently compromise the switch functionality and render it non-functional.

Hardware compatibility for VSP 7200 Series

This section lists the VSP 7200 Series hardware and indicates the software release support.

VSP 7200 hardware

Part number	Model number	Initial release	Supported release	
			4.2.1	5.0
EC720001F-E6	VSP 7254XSQ DC (Front to back airflow)	4.2.1	Y	Y
EC7200x1B-E5 EC7200x1F-E6 B represents back to front airflow. F represents front to back airflow. Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 7254XSQ	4.2.1	Y	Y
EC720002F-E6	VSP 7254XTQ DC (Front to back airflow)	4.2.1	Y	Y
EC7200x2B-E5 EC7200x2F-E6 B represents back to front airflow. F represents front to back airflow. Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 7254XTQ	4.2.1	Y	Y

***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.

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 7200 Series 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 7200 Series 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 7200 Series 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 VSP Operating System Software*, NN47227-301.

VSP 7200 operational notes

- The VSP 7254XSQ has a PHYless design, which is typical for Data Center top of rack switches. The benefits of a PHYless design are lower power consumption and lower latency. However, due to the PHYless design, the following transceivers are not supported:
  - AA1403017-E6: 1-port 10GBASE-LRM SFP+
  - AA1403016-E6: 1-port 10GBase-ZR/ZW SFP+

    The AA1403165 10GBASE-ZR CWDM DDI SFP+ transceiver can be substituted for AA1403016-E6 10GBASE-ZR/ZW SFP+.
- Software partitions the switch into two logical slots: Slot 1 and Slot 2.
  - Slot 1: 10 Gbps ports: 1 - 48
  - Slot 2: 40 Gbps ports: 1 - 6
- Channelization is supported on the 40 Gbps QSFP+ ports.
- MACsec support:
  - MACsec is only supported on the VSP 7254XTQ 10 Gbps ports.
  - MACsec is not supported on VSP 7254XSQ 10 Gbps ports.
  - MACsec is not supported on VSP 7254XTQ and VSP 7254XSQ 40 Gbps ports whether channelization is enabled or not.
- 1000BASE-T SFP (AA1419043-E6) will only operate at 1 Gbps speeds when used on a VSP 7254XSQ.

- When you use 1 Gigabit Ethernet SFP transceivers on VSP 7254XSQ, the software disables auto-negotiation on the port:
    - If you use 1 Gbps fiber SFP transceivers, the remote end must also have auto-negotiation disabled.
    - If you use 1 Gbps copper SFP transceivers, the remote end must have auto-negotiation enabled. If not, the link will not be established.
- When a port on VSP 7254XSQ is disabled or enabled, or a cable replaced, or the switch rebooted, the remote link can flap twice.
- Avaya recommends enabling auto-negotiation to ensure proper operation at 100 Mbps speeds on VSP 7254XTQ:
    - Link instability will be seen if both ends are set to 100 Mbps auto-negotiation disabled and you use a straight through cable.
    - If Link instability is seen when you use a cross-over cable, a port disable or enable can fix the issue.

For more information, see *Installing Transceivers and Optical Components on VSP Operating System Software*, NN47227-301

Hardware compatibility for VSP 8000 Series

This section lists the VSP 8000 Series hardware and indicates the software release support.

Note:

4.1 is the first VOSS release. Release numbers earlier than 4.1 are releases specific to VSP 8000.

Part numbers that end in GS are the TAA-compliant version of the hardware.

VSP 8000 hardware

Part number	Model number	Initial release	Supported release					
			4.0.1	4.0.50	4.1	4.2	4.2.1	5.0
EC8200x01-E6 EC8200x01-E6GS Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 8284XSQ	4.0	Y	Y	Y	Y	Y	Y
EC8200001-E6	VSP 8284XSQ-DC	4.0.50	—	Y	—	—	Y	Y
EC8400001-E6	VSP 8404-DC	4.2.1	—	—	—	—	Y	Y
EC8400x01-E6	VSP 8404	4.2	—	—	—	Y	Y	Y

Table continues…

Part number	Model number	Initial release	Supported release					
			4.0.1	4.0.50	4.1	4.2	4.2.1	5.0
EC8200x01-E6GS Note: Replace the “x” with a country specific power cord code. See the footnote for details.								
Ethernet Switch Modules (ESM) — VSP 8400 only **Important:** Ensure the switch runs, at a minimum, the noted initial software release before you install an ESM.								
EC8404001-E6 EC8404001-E6GS	8424XS	4.2	—	—	—	Y	Y	Y
EC8404002-E6 EC8404002-E6GS	8424XT	4.2	—	—	—	Y	Y	Y
EC8404003-E6 EC8404003-E6GS	8408QQ	4.2	—	—	—	Y	Y	Y
EC8404005-E6 EC8404005-E6GS	8418XSQ	4.2	—	—	—	Y	Y	Y
EC8404006-E6 EC8404006-E6GS	8418XTQ	5.0	—	—	—	—	—	Y
EC8404007-E6 EC8404007-E6GS	8424GS	5.0	—	—	—	—	—	Y
EC8404008-E6 EC8404008-E6GS	8424GT	5.0	—	—	—	—	—	Y
***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.								

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 Series 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 Series 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 Series 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 VSP Operating System Software*, NN47227-301.

Power supply compatibility

You can use certain power supplies in more than one VOSS platform. This section lists the power supplies and indicates the compatible platforms.

For more specific information on each power supply, see the following documents:

- *Installing Avaya Virtual Services Platform 4850GTS Series*, NN46251-300
- *Installing Avaya Virtual Services Platform 4450GTX-HT-PWR+ Switch*, NN46251–304
- *Installing Avaya Virtual Services Platform 4450GSX-PWR+ Switch*, NN46251-307
- *Installing the Avaya Virtual Services Platform 8000 Series*, NN47227-300
- *Installing the Avaya Virtual Services Platform 7200 Series*, NN47228-302

VSP 4000 Series power supplies

Platform	300 W AC AL1905x08-E5	300 W DC AL1905005-E5	1,000 W AC AL1905x21-E6	1,000 W AC-HT EC4005x03-E6HT
VSP 4850GTS-DC	—	Y	—	—
VSP 4850GTS-PWR+	—	—	Y	Y
VSP 4850GTS	Y	—	—	—

Table continues…

Platform	300 W AC AL1905x08-E5	300 W DC AL1905005-E5	1,000 W AC AL1905x21-E6	1,000 W AC-HT EC4005x03-E6HT
VSP 4450GTX-HT-PWR+	—	—	—	Y
VSP 4450GSX-DC	—	Y	—	—
VSP 4450GSX-PWR+	—	—	Y	Y

VSP 7200 Series and VSP 8000 Series power supplies

Platform	460 W AC front-to-back EC7205x1F-E6	460 W AC back-to-front EC7205x1B-E6	800 W AC front-to-back EC8005x01-E6	800 W AC front-to-back EC7205x0F-E6	800 W AC back-to-front EC7205x0B-E6	800 W DC front-to-back EC8005001-E6
VSP 8284XSQ	—	—	Y	—	—	—
VSP 8284XSQ-DC	—	—	—	—	—	Y
VSP 8404	—	—	Y	—	—	—
VSP 8404-DC	—	—	—	—	—	Y
VSP 7254XSQ front-to-back	Y	—	—	—	—	—
VSP 7254XSQ back-to-front	—	Y	—	—	—	—
VSP 7254XTQ front-to-back	—	—	—	Y	—	—
VSP 7254XTQ back-to-front	—	—	—	—	Y	—
VSP 7254XSQ-DC	—	—	—	—	—	Y
VSP 7254XTQ-DC	—	—	—	—	—	Y

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.

Software scaling capabilities

This section lists software scaling capabilities of the following products:

- Avaya Virtual Services Platform 4000 Series
- Avaya Virtual Services Platform 7200 Series
- Avaya Virtual Services Platform 8000 Series

Table 3: Software scaling capabilities

	Maximum number supported		
	VSP 4000 Series	**VSP 7200 Series**	**VSP 8000 Series**
Layer 2			
MAC table size (without SPBM)	32,000	224,000	224,000
MAC table size (with SPBM)	16,000	112,000	112,000
Port based VLANs	4,059	4,059	4,059
Private VLANs (E-Tree)	1,000	4,059	4,059
Protocol based VLANs (IPv6 only)	1	1	1
RSTP instances	1	1	1
MSTP instances	12	12	12
LACP aggregators	50	54 (up to 72 with channelization)	84 (up to 96 with channelization)
Ports per LACP aggregator	8-active	8-active	8-active
MLT groups	50	54 (up to 72 with channelization)	84 (up to 96 with channelization)
Ports per MLT group	8	8	8
SLPP VLANs	128	128	128
VLACP interfaces	50	54 (up to 72 with channelization)	84 (up to 96 with channelization)

Table continues…

	Maximum number supported		
	VSP 4000 Series	**VSP 7200 Series**	**VSP 8000 Series**
FHS RA guard policies	10	10	10
FHS DHCP guard policies	10	10	10
Layer 3 (IPv4 & IPv6 Common)			
IP interfaces (IPv4 or IPv6)	256	506 *See note in the row below	506 *See note in the row below
VRRP interfaces (IPv4/IPv6)	64	252 *See note in the row below	252 *See note in the row below
Routed Split Multi-Link Trunking (RSMLT) interfaces (IPv4 or IPv6)	252	252 *See note in the row below	252 *See note in the row below
VSP 7200 Series and VSP 8000 Series: **Note:** * The number of IP interfaces plus the number of VRRP interfaces plus the number of RSMLT interfaces plus 2 (if IP shortcuts is enabled) should not exceed 508.			
VRRP interfaces with fast timers (200ms) - IPv4/IPv6	24	24	24
ECMP groups/paths per group	500/4	1,000/8	1,000/8
OSPF v2/v3 interfaces	100	500	500
OSPF v2/v3 neighbors (adjacencies)	100	500	500
OSPF areas	12 for each VRF 64 for the switch	12 for each VRF 80 for the switch	12 for each VRF 80 for the switch
Layer 3 (IPv4)			
IPv4 ARP table	6,000	32,000	32,000
IPv4 static ARP entries	200 for each VRF 1,000 for the switch	2,000 for each VRF 10,000 for the switch	2,000 for each VRF 10,000 for the switch
IPv4 CLIP interfaces	64	64	64
IPv4 route table size	16,000	N/A	N/A
IPv4 route table size with "ipv6-mode" boot flag set to false	N/A	16,000	16,000

Table continues…

	Maximum number supported		
	VSP 4000 Series	**VSP 7200 Series**	**VSP 8000 Series**
IPv4 route table size with "ipv6-mode" boot flag set to true	N/A	8,000	8,000
IPv4 static routes	1,000 for each VRF 1,000 for the switch	1,000 for each VRF 5,000 for the switch	1,000 for each VRF 5,000 for the switch
RIP interfaces	24	200	200
IPv4 RIP routes	IPv4 and IPv6 route scaling depends on the combination of the ipv6-mode and urpf-mode boot config flags. For more information, see Table 4: IPv4 and IPv6 route scaling on page 51.		
IPv4 OSPF routes	IPv4 and IPv6 route scaling depends on the combination of the ipv6-mode and urpf-mode boot config flags. For more information, see Table 4: IPv4 and IPv6 route scaling on page 51.		
BGP peers	12	12	12
IPv4 BGP routes	IPv4 and IPv6 route scaling depends on the combination of the ipv6-mode and urpf-mode boot config flags. For more information, see Table 4: IPv4 and IPv6 route scaling on page 51.		
IPv4 shortcut routes	IPv4 and IPv6 route scaling depends on the combination of the ipv6-mode and urpf-mode boot config flags. For more information, see Table 4: IPv4 and IPv6 route scaling on page 51.		
IPv4 route policies	500 for each VRF 5,000 for the switch	500 for each VRF 5,000 for the switch	500 for each VRF 5,000 for the switch
IPv4 NLB interfaces	N/A	256	256
IPv4 VRF instances	24	24	24
IPv4 UDP forwarding	128	512	512
IPv4 DHCP Relay forwarding	128	1,024	1,024
Layer 3 (IPv6)			
IPv6 Neighbor table	4,000	8,000	8,000
IPv6 static neighbor records	128	256	256
IPv6 CLIP interfaces	64	64	64
IPv6 static routes	1,000	1,000	1,000
IPv6 OSPFv3 routes - GRT only	IPv4 and IPv6 route scaling depends on the combination of the ipv6-mode and urpf-mode boot config flags. For more information, see Table 4: IPv4 and IPv6 route scaling on page 51.		
IPv6 shortcut routes – GRT only	IPv4 and IPv6 route scaling depends on the combination of the ipv6-mode and urpf-mode boot config flags. For more information, see Table 4: IPv4 and IPv6 route scaling on page 51.		

Table continues…

	Maximum number supported		
	VSP 4000 Series	**VSP 7200 Series**	**VSP 8000 Series**
IPv6 6in4 configured tunnels	254	506	506
RIPng interfaces	24	48	48
RIPng routes	IPv4 and IPv6 route scaling depends on the combination of the ipv6-mode and urpf-mode boot config flags. For more information, see Table 4: IPv4 and IPv6 route scaling on page 51.		
IPv6 DHCP Relay forwarding	128	512	512
IP Multicast			
IGMP interfaces	4,059	4,059	4,059
PIM interfaces	128 (Active), 256 (Passive)	128 (Active) 500 (Passive)	128 (Active), 500 (Passive)
PIM Neighbors (GRT Only)	128	128	128
PIM-SSM static channels	512	4,000	4,000
Multicast receivers or IGMP joins (per switch)	1,000	6,000	6,000
Multicast senders (per switch)	1,000	6,000	6,000
Total multicast routes (per switch)	4,000	6,000	6,000
Static multicast routes	512	4,000	4,000
Multicast enabled Layer 2 VSN	1,000	2,000	2,000
Multicast enabled Layer 3 VSN	24	24	24
Filters and QoS			
Total IPv4 Ingress rules/ ACEs (Port/VLAN based, Security/QoS filters)	1,530	766	766
Total IPv4 Egress rules/ ACEs (Port based, Security filters)	254	252	252
Total IPv6 Ingress rules/ ACEs (Port/VLAN based, Security/QoS filters)	256	256	256
Diagnostics			
Mirrored ports	49	53 (up to 71 with channelization)	83 (up to 95 with channelization)

Table continues…

	Maximum number supported		
	VSP 4000 Series	**VSP 7200 Series**	**VSP 8000 Series**
OAM			
FTP sessions (IPv4/IPv6)	4	4	4
Rlogin sessions (IPv4/IPv6)	8	8	8
SSH sessions (IPv4/IPv6)	8 total (any combination of IPv4 and IPv6 up to 8)	8 total (any combination of IPv4 and IPv6 up to 8)	8 total (any combination of IPv4 and IPv6 up to 8)
Telnet sessions (IPv4/IPv6)	8	8	8

The following table provides information on IPv4 and IPv6 route scaling. The route scaling does not depend on the protocol itself but rather the general system limitation in the following configuration modes:

- URPF check mode — Enable this flag to support Unicast Reverse Path Forwarding check mode.
- IPv6 mode — Enable this flag to support IPv6 routes with prefix-lengths greater than 64 bits. When the IPv6-mode boot config flag is enabled, the maximum number of IPV4 routing table entries decreases. This flag does not apply to VSP 4000 Series.

Table 4: IPv4 and IPv6 route scaling

URPF check mode	IPv6 mode	VSP 4000 Series			VSP 7200 Series and VSP 8000 Series		
		IPv4	**IPv6**		**IPv4**	**IPv6**	
			Prefix less than or equal to 64	**Prefix greater than 64**		**Prefix less than or equal to 64**	**Prefix greater than 64**
No	No	15,744	7,887	256	15,488	7,744	n/a
No	Yes	n/a	n/a	n/a	7,488	3,744	2,000
Yes	No	7,872	3,943	128	7,744	3,872	n/a
Yes	Yes	n/a	n/a	n/a	3,744	1,872	1,000

Fabric scaling for VSP 4000 Series

The following table provides fabric scaling information.

Table 5: Fabric scaling

Attribute	vIST configured	vIST not configured
Number of SPB regions	1	1

Table continues…

Attribute	vIST configured	vIST not configured
Number of BVIDs	2	2
BCB mode (NNI switching supported yes/no)	Yes	Yes
Layer 2 MAC table size (with SPB)	16,000	16,000
SPBM-enabled switches per region (BEB and BCB)	2,000	2,000
Number of BEBs this node can share services with (Layer 2 VSNs, Layer 3 VSNs, E-Tree, Multicast, Transparent Port UNI). vIST clusters are counted as 3 nodes. Each Fabric Extend ISIS adjacency reduces this number by 1.	2,000	2,000
Number of vIST/IST clusters this node can share I-SIDs with	2,000	2,000
Maximum number of Layer 2 VSNs per switch	1,000	1,000
Maximum number of SPB Layer 2/ Layer 3 multicast UNI I-SIDs (S,G) per switch	1,000 See Table 6: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured on page 53.	1,000 See Table 6: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured on page 53.
Maximum number of Switched UNI I-SIDs per switch	1,000 See Table 6: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured on page 53.	1,000 See Table 6: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured on page 53.
Maximum number of FA ISID/ VLAN assignments per port	94	94
Maximum number of Layer 3 VSNs per switch	24	24
Maximum number of Transparent Port UNI per switch	48	48
Maximum number of E-Tree PVLAN UNI per switch	1,000	1,000
Maximum number of NNI interfaces and adjacencies	VSP 4450 = 255 VSP 4850 = 24	VSP 4450 = 255 VSP 4850 = 24

Table 6: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured

Number of NNI configured	Number of UNI I-SIDs supported (UNI I-SIDs are used for UNI Layer 2 VSN, Layer 3 VSN,T-UNI, E-Tree, Switched-UNI, S,G for multicast) vIST configured	Number of UNI I-SIDs supported (UNI I-SIDs are used for UNI Layer 2 VSN, Layer 3 VSN,T-UNI, E-Tree, Switched-UNI, S,G for multicast) vIST not configured
Number of NNI = 4	1,000	1,000
Number of NNI = 6	1,000	1,000
Number of NNI = 10	650	1,000
Number of NNI = 20	350	700
Number of NNI = 48	150	300
Number of NNI = 72	100	200
Number of NNI = 100	75	150
Number of NNI = 128	60	120
Number of NNI = 250	30	60

Fabric scaling for VSP 7200 Series

The following table provides fabric scaling information.

Table 7: Fabric scaling

Attribute	vIST configured	vIST not configured
Number of SPB regions	1	1
Number of BVIDs	2	2
BCB mode (NNI switching supported yes/no)	Yes	Yes
Layer 2 MAC table size (with SPB)	112,000	112,000
SPBM-enabled switches per region (BEB and BCB)	2,000	2,000
Number of BEBs this node can share services with (Layer 2 VSNs, Layer 3 VSNs, E-Tree, Multicast, Transparent Port UNI). vIST clusters are counted as 3 nodes. Each Fabric Extend ISIS adjacency reduces this number by 1.	500	500

Table continues…

Attribute	vIST configured	vIST not configured
Number of vIST/IST clusters this node can share I-SIDs with	330	330
Maximum number of Layer 2 VSNs per switch	4,059	4,059
Maximum number of SPB Layer 2/ Layer 3 multicast UNI I-SIDs (S,G) per switch	4,000 See Table 8: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured on page 54.	4,000 See Table 8: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured on page 54.
Maximum number of Switched UNI I-SIDs per switch	4,000 See Table 8: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured on page 54.	4,000 See Table 8: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured on page 54.
Maximum number of FA ISID/ VLAN assignments per port	94	94
Maximum number of Layer 3 VSNs per switch	24	24
Maximum number of Transparent Port UNI per switch	54 (up to 72 with channelization)	54 (up to 72 with channelization)
Maximum number of E-Tree PVLAN UNI per switch	4,059	4,059
Maximum number of NNI interfaces and adjacencies	255	255

Table 8: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured

Number of NNI configured	Number of UNI I-SIDs supported (UNI I-SIDs are used for UNI Layer 2 VSN, Layer 3 VSN,T-UNI, E-Tree, Switched-UNI, S,G for multicast) vIST configured	Number of UNI I-SIDs supported (UNI I-SIDs are used for UNI Layer 2 VSN, Layer 3 VSN,T-UNI, E-Tree, Switched-UNI, S,G for multicast) vIST not configured
Number of NNI = 4	4,000	4,000
Number of NNI = 6	3,500	4,000
Number of NNI = 10	2,900	4,000
Number of NNI = 20	2,000	4,000
Number of NNI = 48	1,000	2,000

Table continues…

Number of NNI = 72	750	1,500
Number of NNI = 100	550	1,100
Number of NNI = 128	450	900
Number of NNI = 250	240	480

Fabric scaling for VSP 8000 Series

The following table provides fabric scaling information.

Fabric scaling

Attribute	vIST configured	vIST not configured
Number of SPB regions	1	1
Number of BVIDs	2	2
BCB mode (NNI switching supported yes/no)	Yes	Yes
Layer 2 MAC table size (with SPB)	112,000	112,000
SPBM-enabled switches per region (BEB and BCB)	2,000	2,000
Number of BEBs this node can share services with (Layer 2 VSNs, Layer 3 VSNs, E-Tree, Multicast, Transparent Port UNI). vIST clusters are counted as 3 nodes. Each Fabric Extend ISIS adjacency reduces this number by 1.	500	500
Number of vIST/IST clusters this node can share I-SIDs with	330	330
Maximum number of Layer 2 VSNs per switch	4,059	4,059
Maximum number of SPB Layer 2/ Layer 3 multicast UNI I-SIDs (S,G) per switch	4,000 See Table 9: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured on page 56.	4,000 See Table 9: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured on page 56.
Maximum number of Switched UNI I-SIDs per switch	4,000 See Table 9: Number of I-SIDs supported depending on the number of IS-IS interfaces and	4,000 See Table 9: Number of I-SIDs supported depending on the number of IS-IS interfaces and

Table continues…

Attribute	vIST configured	vIST not configured
	adjacencies (NNI) configured on page 56.	adjacencies (NNI) configured on page 56.
Maximum number of FA ISID/ VLAN assignments per port	94	94
Maximum number of Layer 3 VSNs per switch	24	24
Maximum number of Transparent Port UNI per switch	84 (up to 96 with channelization)	84 (up to 96 with channelization)
Maximum number of E-Tree PVLAN UNI per switch	4,059	4,059
Maximum number of NNI interfaces and adjacencies	255	255

Table 9: Number of I-SIDs supported depending on the number of IS-IS interfaces and adjacencies (NNI) configured

Number of NNI configured	Number of UNI I-SIDs supported (UNI I-SIDs are used for UNI Layer 2 VSN, Layer 3 VSN,T-UNI, E-Tree, Switched-UNI, S,G for multicast) vIST configured	Number of UNI I-SIDs supported (UNI I-SIDs are used for UNI Layer 2 VSN, Layer 3 VSN,T-UNI, E-Tree, Switched-UNI, S,G for multicast) vIST not configured
Number of NNI = 4	4,000	4,000
Number of NNI = 6	3,500	4,000
Number of NNI = 10	2,900	4,000
Number of NNI = 20	2,000	4,000
Number of NNI = 48	1,000	2,000
Number of NNI = 72	750	1,500
Number of NNI = 100	550	1,100
Number of NNI = 128	450	900
Number of NNI = 250	240	480

File names for VOSS 5.0

This section lists the software files for the following VOSS platforms:

- VSP 4000 Series
- VSP 7200 Series
- VSP 8000 Series

⚠ **Caution:**

To download the software files, use Mozilla Firefox. Do not use Internet Explorer or Google Chrome to download software files.

Download images using the binary file transfer.

Check that the file type suffix is `.tgz` and that the image names after you download them to the device match those shown in the following table. Some download utilities append `.tar` to the file name or change the filename extension from `.tgz` to `.tar`. If the file type suffix is `.tar` or the filename does not exactly match the names shown in the preceding table, rename the downloaded file to the name shown in the table so that the activation procedures operate properly.

❗ **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 58. 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 59. On a Windows machine, use the appropriate Windows utility that is supported on your Windows version.

Starting in VOSS 4.2, the encryption modules are included as part of the standard runtime software image file.

Prior to VOSS 4.2.1, image filenames began with VSP, for example, VSP4K4.1.0.0.tgz. In VOSS 4.2.1 and later, image filenames start with VOSS, for example, VOSS8K4.2.1.0.tgz.

The following table lists the files for this release.

Table 10: VSP 4000 file names and sizes

Description	File name	Size (in bytes)
Standard runtime software image	VOSS4K.5.0.0.0.tgz	112,598,210
MIB files	• VOSS4K.5.0.0.0_mib.zip • VOSS4K.5.0.0.0_mib.txt	• 975,311 • 6,538,777
Supported MIB object names	VOSS4K.5.0.0.0_mib_sup.txt	943,502
EDM Help	VSP4000v500_HELP_EDM_gzip.zip	2,815,973
EDM plug-in for COM	VSP4000v5.0.0.0.zip	4,234,180
Logs reference	VOSS4K.5.0.0.0_edoc.tar	59,555,840

Table 11: VSP 7200 file names and sizes

Description	File name	Size (in bytes)
Standard runtime software image	VOSS7K.5.0.0.0.tgz	61,568,786
MIB files	• VOSS7K.5.0.0.0_mib.zip • VOSS7K.5.0.0.0_mib.txt	• 975,311 • 6,538,777

Table continues…

Description	File name	Size (in bytes)
Supported MIB object names	VOSS7K.5.0.0.0_mib_sup.txt	937,561
EDM Help	VOSSv500_HELP_EDM_gzip.zip	2,839,094
EDM plug-in for COM	VOSSv5.0.0.0.zip	4,323,622
Logs reference	VOSS7K.5.0.0.0_edoc.tar	59,555,840

Table 12: VSP 8000 file names and sizes

Description	File name	Size (in bytes)
Standard runtime software image	VOSS8K.5.0.0.0.tgz	61,567,903
MIB files	• VOSS8K.5.0.0.0_mib.zip • VOSS8K.5.0.0.0_mib.txt	• 975,311 • 6,538,777
Supported MIB object names	VOSS8K.5.0.0.0_mib_sup.txt	937,561
EDM Help	VOSSv500_HELP_EDM_gzip.zip	2,839,094
EDM plug-in for COM	VOSSv5.0.0.0.zip	4,323,622
Logs reference	VOSS8K.5.0.0.0_edoc.tar	59,555,840

Open Source software files

The following table lists the details of the Open Source software files distributed with the switch software.

Table 13: Open Source software files

Product	Master copyright file	Open source base software for 5.0
VSP 4000 Series	VOSS4K.5.0.0.0_oss-notice.html	VOSS4K.5.0.0.0_OpenSource.zip
VSP 7200 Series	VOSS7K.5.0.0.0_oss-notice.html	VOSS7K.5.0.0.0_OpenSource.zip
VSP 8000 Series	VOSS8K.5.0.0.0_oss-notice.html	VOSS8K.5.0.0.0_OpenSource.zip

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  VSP8200.4.0.0.0_edoc.tar
d000965876dee2387f1ca59cf081b9d6  VSP8200.4.0.0.0_mib.txt
897303242c30fd944d435a4517f1b3f5  VSP8200.4.0.0.0_mib.zip
2fbd5eab1c450d1f5feae865b9e02baf  VSP8200.4.0.0.0_modules.tgz
a9d6d18a979b233076d2d3de0e152fc5  VSP8200.4.0.0.0_OpenSource.zip
8ce39996a131de0b836db629b5362a8a  VSP8200.4.0.0.0_oss-notice.html
80bfe69d89c831543623aaad861f12aa  VSP8200.4.0.0.0.tgz
a63a1d911450ef2f034d3d55e576eca0  VSP8200v4.0.0.0.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  VSP8200.4.0.0.0.tgz
-rw-r--r--  1 0       0          44208471 Dec  8 08:19  VSP8200.4.0.1.0.tgz
Switch:1>md5 VSP8200.4.0.0.0.tgz
MD5 (VSP8200.4.0.0.0.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.4.0.40.0.tgz

02c7ee0570a414becf8ebb928b398f51 VSP4K.4.0.40.0.tgz
```

View the md5 checksum of the software suite:

```
$ more VSP4K.4.0.40.0.md5
285620fdc1ce5ccd8e5d3460790c9fe1 VSP4000v4.0.40.0.zip

a04e7c7cef660bb412598574516c548f VSP4000v4040_HELP_EDM_gzip.zip
ac3d9cef0ac2e334cf94799ff0bdd13b VSP4K.4.0.40.0_edoc.tar
29fa2aa4b985b39843d980bb9d242110 VSP4K.4.0.40.0_mib_sup.txt
c5f84beaf2927d937fcbe9dd4d4c7795 VSP4K.4.0.40.0_mib.txt
ce460168411f21abf7ccd8722866574c VSP4K.4.0.40.0_mib.zip
1ed7d4cda8b6f0aaf2cc6d3588395e88 VSP4K.4.0.40.0_modules.tgz
1464f23c99298b80734f8e7fa32e65aa VSP4K.4.0.40.0_OpenSource.zip
945f84cb213f84a33920bf31c091c09f VSP4K.4.0.40.0_oss-notice.html
02c7ee0570a414becf8ebb928b398f51 VSP4K.4.0.40.0.tgz
```

Best practices for SPB regarding MSTP

Avaya recommends that NNI ports be used exclusively to transport traffic for SPB-based services and not be configured as members of any VLANs other than SPB BVLANs. Currently, when an IS-IS interface is created on an NNI port or an MLT, MSTP is automatically disabled for MSTI-62 on the port/MLT. But MSTP is not automatically disabled on the NNI ports for the CIST (default MSTI). Avaya recommends that the MSTP be completely disabled on the NNI ports. The following command can be used to disable MSTP completely on the NNI ports.

```
interface gigabitEthernet <port>
no spanning-tree mstp
```

Coexistence of MSTP and SPB based services on NNI ports:

In order to support the coexistence of Non-SPB based services on the NNI ports, the software currently permits adding NNI ports as members of VLANs other than BVLANs. These other VLANs rely on the use of MSTP for Loop prevention. The network operator has to carefully consider the implication of any decision to leave MSTP enabled on the NNI ports. Any MSTP topology changes detected on the NNI ports will impact all services and cause most dynamically learned information on the UNI side to be flushed and relearned. This includes, but is not limited to, all customer MAC and ARP records. This can also cause all the UNI ports on a BEB to be temporarily put into a spanning-tree blocking state before transitioning to a forwarding state again. The net result of this is that MSTP topology changes on the NNI ports adversely impact traffic for SPB based services. For this reason Avaya strongly recommends that the NNI ports be used exclusively for SPB traffic.

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
```

Supported browsers

The switch supports the following browsers to access Enterprise Device Manager (EDM):

- Microsoft Internet Explorer 8.0
- Mozilla Firefox 42

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 the following documents:

- For the VSP 7200 Series and VSP 8000 Series, see *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600.
- For the VSP 4000 Series, see *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600.

Security modes

The VOSS platforms support three security modes:

- Enhanced secure
- Hsecure
- SSH secure

Enable SSH secure mode to allow only SSH to be used and disable all other protocols which include Telnet, rlogin, FTP, SNMP, TFTP, HTTP, and HTTPS. Enabling this mode disables Telnet, rlogin, FTP, SNMP, TFTP, HTTP, and HTTPS by setting the boot flags for these protocols to off. You can over-ride the configuration and enable required protocols individually for run-time use. The administrator will have to enable required protocols individually for run-time use again following a reboot even if you save the configuration. This is because the SSH secure mode enable takes precedence at the time of reboot and the other protocols will be disabled even though the configuration file has them set to enabled.

Note:

Disabling SSH secure mode will not automatically enable the OA&M protocols that were disabled. The boot flags for the required protocols will have to be individually set to enabled.

The following table lists the differences between enhanced secure mode and hsecure mode.

Table 14: Enhanced secure mode versus hsecure mode

Feature	Enhanced secure	Hsecure
Authentication	Role-based: • admin • privilege • operator • security • auditor	Access-level based: • rwa • rw • ro • l3 • l2 • l1
Password length	Minimum of 8 characters with the exception of the Admin, which requires a minimum of 15 characters	10 characters, minimum
Password rules	1 or 2 upper case, lower case, numeric and special characters	Minimum of 2 upper case, 2 lower case, 2 numeric and 2 special characters
Password expiration	Per-user minimum change interval is enforced, which is programmed by the Administrator	Global expiration, configured by the Admin
Password-unique	Previous passwords and common passwords between users are prevented	The same
Password renewal	Automatic password renewal is enforced	The same
Audit logs	Audit logs are encrypted, and authorized users are able to view, modify, and delete.	Standard operation
SNMPv3	Password rules apply to SNMPv3 Auth&Priv. SNMPv3 is required (V1/V2 disabled)	SNMPv1 and SNMPv2 can be enabled.
EDM	Site Admin to enable or disable	Disabled
Telnet and FTP	Site Admin to enable or disable	The same

Table continues…

Feature	Enhanced secure	Hsecure
DOS attack Prevention	Not available	Prevents DOS attacks by filtering IP addresses and IP address ranges.

Feature licensing

After you start a new system, the 60–day Premium Trial license countdown begins. You will see notification messages as the countdown approaches the end of the trial period. After 60 days, the Premium Trial license expires. You will see messages on the console and in the alarms database that the license has expired. The next time you restart the system after the license expiration, the system no longer supports Premier services.

If you use a Base License, you do not need to install a license file. 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 how to install a license file, see the following documents:

- For information on the VSP 4000 Series, see *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 .
- For information on the VSP 7200 Series and VSP 8000 Series, see *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600.

Important:

The license filename stored on a device must meet the following requirements:

- Maximum of 63 alphanumeric characters
- No spaces or special characters allowed
- Underscore (_) is allowed
- The file extension ".xml" is required

SFP+ ports

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

For a complete list of supported SFPs and QSFPs, see *Installing Transceivers and Optical Components on VSP Operating System Software*, NN47227-301.

LACP with Simplified vIST/SPB NNI links

LACP is not recommended on SPB NNI MLT links or on the Simplified Virtual IST.

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.
```

show vlan remote-mac-table command output

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 B-MAC, 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.

dos-chkdsk

If at the end of the **`dos-chkdsk WORD<1-99>`** command output you see:

```
1) Correct
2) Don't correct
```

Then, you should run the **`dos-chkdsk WORD<1-99> repair`** command.

Auto negotiation settings

VOSS 4.1 and later software requires the same auto negotiation settings on link partners to avoid incorrect declaration of link status. Mismatched settings can cause the links to stay down as well as unpredictable behavior. Ensure the auto negotiation settings between local ports and their remote link partners match before upgrading software to VOSS 4.1 or later.

Interoperability notes for Fabric Attach

For Fabric Attach to operate between a VOSS platform and an ERS device, the ERS device must meet minimum software requirements. The following tables identify the minimum GA software releases required to build an FA solution.

Table 15: Extending Fabric using Static FA Proxy configuration (ISID/VLAN is manually configured on FA Proxy)

FA Server		FA Proxy	
Product	**Minimum release**	**Product**	**Minimum release**
VSP 4000 VSP 7200 VSP 8200 VSP 8400	5.0.0.0	ERS 5900	7.0.1
		ERS 5600	6.6.3
		ERS 4800	5.9.2
		ERS 4500	5.7.3

Table 16: Extending Fabric to FA Clients by using FA Proxy

FA Server		FA Proxy		FA Policy	FA Client	
Product	**Minimum release**	**Product**	**Minimum release**		**Product**	**Minimum release**
VSP 4000 VSP 7200 VSP 8200 VSP 8400	5.0.0.0	ERS 5900	7.0.1	IDE Release 9.1 (See Note below)	AP9100	7.2.5
		ERS 5600	6.6.3			
		ERS 4800	5.9.2			
		ERS 4500	5.7.3			

Note:

Required for AP9100 FA Client. IDE sends FA ISID/VLAN assignment request by using FA Proxy to VOSS FA Server.

Interoperability considerations for IS-IS external metric

Support for the `external` metric in IS-IS is new to VOSS release 5.0. BEBs running VOSS 5.0 can advertise routes into IS-IS with the metric type as external. They can also correctly interpret routes advertisements with metric type external received via IS-IS. In an SPB network with a mix of product types running different versions of software releases, care must to be taken to ensure that turning on the ability to use metric-type external does not cause unintended loss of connectivity.

Important:

Note the following before turning on IS-IS external metric if the SPB network has switches running a release other than VOSS 5.0.

- There are no special release or product type implications if the switch does not have IP shortcuts or L3VSN enabled. For example, this applies to L2 only BEBs and BCBs.
- There are no special release or product type implications if the L3VSN in which routes are being advertised with a metric-type of external is not configured on the switch.
- If a switch running a VOSS release that is prior to VOSS 5.0 but VOSS 4.2.1 or later, it will treat all IS-IS routes as having metric-type `internal`, irrespective of the metric-type (internal or external) used by the advertising BEB in its route advertisement.
- Switches running VSP 9000 release 4.1.0.0 or later will treat all IS-IS routes as having metric-type `internal`, irrespective of the metric-type (internal or external) used by the advertising BEB in its route advertisement.
- Switches running VOSS releases prior to 4.2.1.0 may not correctly install IS-IS routes in a L3VSN if any routes are advertised with metric-type external are advertised in that L3VSN by other BEBs in the network. L3VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to GRT.
- Switches running VSP 9000 releases prior to 4.1.0.0 may not correctly install IS-IS routes in a L3VSN if any routes are advertised with metric-type external are advertised in that L3VSN by other BEBs in the network. L3VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to GRT.
- Switches running any ERS 8800 release may not correctly install IS-IS routes in of a L3VSN if any routes are advertised with metric-type external are advertised in that L3VSN by other BEBs in the network. L3VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to GRT.

VSP 4000 specific notices

Converting ERS 4850 to VSP 4000

This section lists information on Avaya switch conversion supported in this release.

Important:

Switch conversion is applicable only to the Avaya Virtual Services Platform 4000 Series. Currently, only the conversion of an Avaya ERS 4850 switch to a VSP 4000 switch is supported.

ERS 4850 and VSP 4000 quick conversion

You can convert an Avaya ERS 4850 switch to a VSP 4000 switch, if there is a network requirement. Avaya provides a conversion kit to convert a single installation (not stacked) of an Avaya ERS 4850 switch to a VSP 4000 switch.

The ERS 4850 to VSP 4000 conversion kit (part number EC4810003.3.0) contains:

- VSP 4000 USB FLASH drive with software module (Release 3.0)
- VSP 4000 USB cover
- Stacking port cover and screws
- 60–day trial license for the VSP 4000

USB considerations for factory supplied and converted VSP 4000 switches

⚠ **Warning:**

The USB FLASH drive on all models of VSP 4850 (factory built and converted from ERS4850) must be treated as a permanent non-removable part of the switch and must NEVER be removed from the switch to ensure proper operation. Additionally, the USB cover must be installed to ensure additional protection against removal. The USB FLASH drive on the VSP 4850 switch is uniquely and permanently bound to the operating system of the switch it is first used on and cannot be transferred to a different switch. Removal (and reinsertion) of the USB FLASH drive from the switch is not supported as it can permanently compromise the switch functionality and render it non-functional.

On a converted VSP 4000 switch, you can also perform a conversion back to the ERS 4850, using the ACLI.

For the conversion to be successful, you must ensure that the hardware and software criteria on the system being converted, are satisfied. For more information, see *ERS 4850 to VSP 4000 Quick Conversion*, NN46251-400.

Interoperability notes for VSP 4000 connecting to an ERS 8800

- For customers running version 7.1.x: The minimum software release is 7.1.3.1, however the recommended ERS 8800 software release is 7.1.5.4 or later. On switches using 8612 XLRS or 8812XL modules for the links connecting to the VSP 4000 the minimum software version is 7.1.5.4. The “spbm version” on the ERS 8800 must be set to “802.1aq”.
- For customers running version 7.2.x: The minimum software release is 7.2.0.2, however the recommended ERS 8800 software release is 7.2.1.1 or later. On switches using 8612 XLRS or 8812XL modules for the links connecting to the VSP 4000 the minimum software version is 7.2.1.1.
- Diffserv is enabled in the VSP 4000 port settings, and is disabled in the ERS 8800 port settings, by default.

Notes on combination ports for VSP 4000

When the VSP 4000 is reset, the peer connections for all ports, including combination ports 47 and 48 on VSP 4450GTX-HT-PWR+, will transition down. During the reset, the fiber ports remain down, but only the copper ports 47 and 48 come up periodically throughout the reset. The copper ports 47 and 48 come up approximately 15 seconds into the reset, remain up for approximately 60 seconds, and then transition down until the boot sequence is complete and all ports come back up.

The following is an example of the status of the combination ports during reset.

```
CP1  [03/18/70 09:55:35.890] 0x0000c5e7 00300001.238 DYNAMIC SET GlobalRouter HW INFO Link
Down(1/47)
CP1  [03/18/70 09:55:35.903] 0x0000c5e7 00300001.239 DYNAMIC SET GlobalRouter HW INFO Link
Down(1/48)

CP1  [03/18/70 09:55:49.994] 0x0000c5ec 00300001.239 DYNAMIC CLEAR GlobalRouter HW INFO
Link Up(1/48)
CP1  [03/18/70 09:55:50.322] 0x0000c5ec 00300001.238 DYNAMIC CLEAR GlobalRouter HW INFO
Link Up(1/47)

CP1  [03/18/70 09:56:43.131] 0x0000c5e7 00300001.238 DYNAMIC SET GlobalRouter HW INFO Link
Down(1/47)
CP1  [03/18/70 09:56:43.248] 0x0000c5e7 00300001.239 DYNAMIC SET GlobalRouter HW INFO Link
Down(1/48)
```

Cabled connections for both copper and fiber ports

The following limitations apply when the combination ports have cabled connections for both the copper and fiber ports.

- Do not use the fiber port and do not insert an SFP into the optical module slot in the following situations:
  - a copper speed setting of either 10M or 100M is required
  - a copper duplex setting of half-duplex is required

Note:

These limitations are applicable only when auto-negotiation is disabled. To avoid this limitation, use auto-negotiation to determine the speed to 10/100/1000 and to determine the duplex.

- The 100M-FX SFP requires auto-negotiation to be disabled. Therefore, auto-negotiation will also be disabled for the copper port. Configure peer switch to disable auto-negotiation.

Chapter 4: Software Upgrade

Image upgrade fundamentals

This section details what you must know to upgrade the switch.

Upgrades

Install new software upgrades to add functionality to the switch. Major and minor upgrades are released depending on how many features the upgrade adds or modifies.

Upgrade time requirements

Image upgrades take less than 30 minutes to complete. The switch continues to operate during the image download process. A service interruption occurs during the installation and subsequent reset of the device. The system returns to an operational state after a successful installation of the new software and device reset.

Before you upgrade the software image

Before you upgrade the switch, ensure that you read the entire upgrading procedure.

You must keep a copy of the previous configuration file (*config.cfg*), in case you need to return to the previous version. The upgrade process automatically converts, but does not save, the existing configuration file to a format that is compatible with the new software release. The new configuration file may not be backward compatible.

Image naming conventions

The switch software use a standardized dot notation format.

Software images

Software images use the following format:

Product Name.Major Release.Minor Release.Maintenance Release.Maintenance Release Update.tgz

For example, the image file name **VOSS4K.4.2.1.0.tgz** denotes a software image for the VSP 4000 product with a major release version of 4, a minor release version of 2, a maintenance release version of 1 and a maintenance release update version of 0. Similarly, the image file name **VSP4K.3.0.1.0.tgz** denotes a software image for the VSP 4000 product with a major release version of 3, a minor release version of 0, a maintenance release version of 1 and a maintenance release update version of 0. TGZ is the file extension.

Interfaces

You can apply upgrades to the switch using the Avaya Command Line Interface (ACLI).

For more information about ACLI, see *Using ACLI and EDM on VSP Operating System Software*, NN47227-103.

File storage options

This section details what you must know about the internal boot and system flash memory and Universal Serial Bus (USB) mass-storage device, which you can use to store the files that start and operate the switch.

The switch file system uses long file names.

Internal flash

The switch has two internal flash memory devices: the boot flash memory and the system flash memory. The system flash memory size is 2 gigabytes (GB).

Boot flash memory is split into two banks that each contain a different copy of the boot image files. Only the Image Management feature can make changes to the boot flash.

The system flash memory stores configuration files, runtime images, the system log, and other files. You can access files on the internal flash through the /intflash/ folder.

USB device

The switch can use a USB device for additional storage or configuration files, release images, and other files. The USB device provides a convenient, removable mechanical to copy files between a computer and a switch, or between switches. In cases where network connectivity has not yet been established, or network file transfer is not feasible, you can use a USB device to upgrade the configuration and image files on the switch.

❗ **Important:**

For VSP 4850, the use of the USB port for file transfers using removable FLASH drive is not supported because the USB FLASH drive on all models of VSP 4850 (factory built and converted from ERS 4850) must be treated as a permanent non-removable part of the switch and must NEVER be removed from the switch to ensure proper operation.

File Transfer Protocol

You can use File Transfer Protocol (FTP) to load the software directly to the switch, or to download the software to the internal flash memory or to an installed USB device.

The switch can act as an FTP server or client. If you enable the FTP daemon (ftpd), you can use a standards-based FTP client to connect to the Control Processor (CP) module by using the ACLI log on parameters. Copy the files from the client to either the internal flash memory or USB device.

Supported upgrade paths

See the following tables for information about supported upgrade paths.

Table 17: Supported upgrade paths on the VSP 4850GTS and VSP 4850GTS-PWR+

Upgrade path	Support
Upgrade from 4.1 to 5.0	Supported
Upgrade from 4.2 to 5.0	Supported
Upgrade from 4.2.1 to 5.0	Supported

Table 18: Supported upgrade paths on the VSP 4450GSX-PWR+

Upgrade path	Support
Upgrade from 4.1 to 5.0	Supported
Upgrade from 4.2 to 5.0	Supported
Upgrade from 4.2.1 to 5.0	Supported

Table 19: Supported upgrade paths on the VSP 4450GTX-HT-PWR+

Upgrade path	Support
Upgrade from 4.1 to 5.0	Supported
Upgrade from 4.2 to 5.0	Supported
Upgrade from 4.2.1 to 5.0	Supported

Table 20: Supported upgrade paths on the VSP 8284XSQ

Upgrade path	Support
Upgrade from 4.1 to 5.0	Supported
Upgrade from 4.2 to 5.0	Supported
Upgrade from 4.2.1 to 5.0	Supported

Table 21: Supported upgrade paths on the VSP 8404

Upgrade path	Support
Upgrade from 4.2 to 5.0	Supported
Upgrade from 4.2.1 to 5.0	Supported

Table 22: Supported upgrade paths on the VSP 7254XSQ and VSP 7254XTQ

Upgrade path	Support
Upgrade from 4.2.1 to 5.0	Supported

Pre-upgrade instructions for IS-IS metric type

The command used to redistribute routes into IS-IS supports an option called `metric-type`, which can take one of two values **internal** or **external**. Prior to VOSS release 5.0, the routes were always advertised into IS-IS as **internal** irrespective of whether the user set the metric-type to **internal** or **external**. The saved configuration itself correctly shows the value that the user selected. Both options of this command are fully supported in VOSS 5.0. If the current configuration file has redistribution commands that set the metric-type to **external**, after upgrading to VOSS release 5.0, the routes will be advertised into IS-IS as external routes. This effectively constitutes a change in how the routes are advertised into IS-IS after the upgrade compared to before the upgrade. This can cause unintended traffic issues if the other switches in the network are not yet upgraded to a release that recognizes external routes in IS-IS.

To avoid unintentionally impacting traffic immediately following an upgrade, it is recommended that the existing IS-IS redistribution configuration of a switch be checked prior to the upgrade to determine if the metric-type is set to **external** in the redistribution commands. If metric-type **external** is not used in the redistribution, the switch can be upgraded using the normal upgrade procedures. If the metric-type **external** is used with any redistribution command, it should be changed to **internal** and the configuration should be saved. After this the switch can be upgraded using the normal upgrade procedures.

Commands to check metric-type in redistribution configuration:

```
Switch:1(config-isis)#show ip isis redistribute [vrf <vrfName>]
================================================================================
  ISIS Redistribute List - GlobalRouter
================================================================================
SOURCE MET MTYPE      SUBNET   ENABLE LEVEL  RPOLICY
--------------------------------------------------------------------------------
RIP    0   internal   allow    TRUE   l1
OSPF   0   external   allow    TRUE   l1
LOC    0   external   allow    TRUE   l1
```

Commands to change metric-type to internal for GRT:

```
router isis
isis redistribute <protocol> metric-type internal
save config
```

The *protocol* above could be one of **direct**, **ospf**, **static**, **rip** or **bgp**.

Commands to change metric-type to internal for VRF:

```
router vrf <vrfName>
isis redistribute <protocol> metric-type internal
save config
```

The *protocol* above could be one of **direct**, **ospf**, **static**, **rip** or **bgp**.

Important upgrade consideration

Starting with VOSS 5.0 release, support for the replay-protect option within MACsec configuration has been removed. The replay-protect option is no longer visible or configurable in VOSS 5.0. If the replay-protect option has been configured, follow the steps mentioned below to carefully disable replay-protect before you upgrade to VOSS 5.0.

✱ **Note:**

Replay-protect must be carefully disabled on both ends of the MACsec enabled link.

Use the **`show macsec status`** command to check if replay-protect has been enabled on any of the interfaces.

For each interface where MACsec replay protect is enabled, perform the following tasks:

1. Disable MACsec replay-protect on the remote end of the MACsec enabled the link.
2. Disable MACsec replay-protect on the local end of the MACsec enabled link.
3. Save the configuration on both nodes.
4. Start the upgrade to VOSS 5.0.

If replay-protect is not disabled on the remote end of the MACsec link prior to the upgrade of the local node to VOSS 5.0, traffic on the MACsec enabled links will be dropped until replay-protect is also disabled on the remote node. As such, it is strongly recommended to follow the above procedure before initiating upgrade to VOSS 5.0.

Saving the configuration

Save the configuration

- When you make a change to the configuration.
- To create a backup configuration file before you upgrade the software on the switch.

After you change the configuration, you must save the changes on the device. Save the configuration to a file to retain the configuration settings.

About this task

File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support IPv4 and IPv6 addresses.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Save the running configuration:

   ```
   save config [backup WORD<1-99>] [file WORD<1-99>] [verbose]
   ```

Example

```
Switch:1> enable
```

Save the configuration to the default location:

```
Switch:1# save config
```

Identify the file as a backup file and designate a location to save the file:

```
Switch:1# save config backup /usb/PreUpgradeBackup.cfg
```

Variable definitions

Use the data in the following table to use the **`save config`** command.

Variable	Value
backup *WORD<1–99>*	Saves the specified file name and identifies the file as a backup file. *WORD<1–99>* uses one of the following format: • a.b.c.d:<file> • /intflash/<file> • /usb/<file> The file name, including the directory structure, can include up to 99 characters.
file *WORD<1–99>*	Specifies the file name in one of the following format: • a.b.c.d:<file> • /intflash/<file> • /usb/<file> The file name, including the directory structure, can include up to 99 characters.
verbose	Saves the default and current configuration. If you omit this parameter, the command saves only parameters you change.

Upgrading the software

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

Use one of the following options to upload the file with the new software to the switch:

- Use FTP or SFTP to transfer the file.
- Download the file to your computer. Copy the file to a USB device and insert the USB device into the USB port on the switch.

Important:

For VSP 4850, the use of the USB port for file transfers using removable FLASH drive is not supported because the USB FLASH drive on all models of VSP 4850 (factory built and converted from ERS 4850) must be treated as a permanent non-removable part of the switch and must NEVER be removed from the switch to ensure proper operation.

You can store up to six software releases on the switch. If you have six releases already stored on the switch, then you will be prompted to remove one release before you can proceed to add and activate a new software release.

For information about how to remove a software release, see Deleting a software release on page 81.

Before you begin

- To obtain the new software, go to the Avaya support site: www.avaya.com/support. You need a valid user or site ID and password.
- Back up the configuration files.
- Use an FTP or SFTP application or USB device to transfer the file with the new software release to the switch.
- Ensure that you have not configured a VLAN above 4059. If you have, you must port all configuration on this VLAN to another VLAN, before you begin the upgrade.

  Caution:

  Starting from Release 3.1, only VLAN range 2 to 4059 is supported. All configuration on a higher numbered VLAN from previous releases will be lost after the upgrade.
- Check the MACsec configuration on the device prior to upgrading to Release 5.0. For more information, see Important upgrade consideration on page 73.
- If you plan to upgrade from either Release 4.2.1.0 or 4.2.1.1 to 5.0 and have IS-IS-enabled links with HMAC-MD5 authentication, use the `no isis hello-auth` command to disable IS-IS authentication one link at a time for all systems. Ensure each link is stable before you move on to the next link. After you have disabled all IS-IS authentication, save the configuration, and then perform the upgrade to 5.0. After the upgrade to 5.0 is complete, you can reenable IS-IS authentication one link at a time, and then save the configuration on each switch.

Note:

Software upgrade configurations are case-sensitive.

About this task

Important:

When both IPv6 `dhcp-relay fwd-path` and IPv6 VRRP are configured on a device that runs 4.1 or 4.2 and you save the configuration, the configuration is saved with an `exit` command missing. This omission prevents the DHCP Relay configuration from loading while rebooting or sourcing the configuration. This issue is fixed in Release 4.2.1, however the omission still exists in configuration files saved using 4.1 or 4.2. As a result, if you upgrade from Release 4.1 or 4.2 to 4.2.1 or later with IPv6 VRRP and IPv6 DHCP configured, the IPv6 DHCP configurations will be lost. After the upgrade, reconfigure IPv6 VRRP- and IPv6 DHCP-related parameters, and then save the configuration. The newer release configuration includes the additional **`exit`** command when saved.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. If you are using the USB port to transfer files, go to the next step. If you are using FTP or SFTP to download the files, start the FTP daemon on the switch and enable the ftpd flag for FTP or sshd flag for SFTP:

   Note:

   Start an FTP session from your computer to the VSP switch using the same username and password used to Telnet or SSH to the switch. Upload or copy the VOSS image (e.g. VOSS4K.5.0.0.0.tgz) to the VSP switch.

   ```
   boot config flag <ftpd | sshd>
   ```

   ```
   end
   ```

3. Download the files to the switch through FTP or SFTP, or transfer them to the switch through the USB port.

4. Enter Privileged EXEC configuration mode by exiting the Global Configuration mode.

   ```
   exit
   ```

5. Extract the release distribution files to the `/intflash/release/` directory:

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

6. Install the image:

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

7. Restart the switch:

   ```
   reset
   ```

   Important:

   After you restart the system, 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. By default, auto-commit is enabled.

8. After you restart the switch, enter Privileged EXEC configuration mode:

   rwa

   ```
   enable
   ```

9. Confirm the software is upgraded:

   `show software`

10. Commit the software:

    `software commit`

Example

The following example is for the VSP 8000, but the same steps apply to other VOSS switches.

```
Switch:1>enable

Switch:1#configure terminal

Switch:1(config)#boot config flags ftpd

Switch:1(config)#end

Switch:1(config)#copy /usb/VOSS8K.5.0.0.0.tgz /intflash/VOSS8K.
5.0.0.0.tgz

Switch:1(config)#exit

Switch:1#software add VOSS8K.5.0.0.0.tgz

Switch:1#software activate VOSS8K.5.0.0.0.GA

Switch:1#reset
```

```
Switch:1#show software
===============================================================================
                    software releases in /intflash/release/
===============================================================================
VOSS8K.5.0.0.0.GA (Primary Release)
VOSS8K.4.2.1.0.GA (Backup Release)

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

Switch:1#show software detail

===============================================================================
                    software releases in /intflash/release/
===============================================================================
VOSS8K.4.2.1.0.GA (Backup Release)
    KERNEL                              2.6.32_int38
    ROOTFS                              2.6.32_int38
    APPFS                               VOSS8K.4.2.1.0int012
  AVAILABLE ENCRYPTION MODULES
    3DES
    AES/DES


VOSS8K.5.0.0.0.GA (Primary Release)
    KERNEL                              2.6.32_int38
    ROOTFS                              2.6.32_int38
    APPFS                               VOSS8K.5.0.0.0.GA
  AVAILABLE ENCRYPTION MODULES
    3DES
    AES/DES
```

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

```
Switch:1#software commit
```

Verifying the upgrade

Verify your upgrade to ensure proper switch operation.

Procedure

1. Check for alarms or unexpected errors:

   `show logging file tail`

2. Verify all modules and slots are online:

   `show sys-info`

Committing an upgrade

Perform the following procedure to commit an upgrade.

About this task

The commit function for software upgrades allows maximum time set by the commit timer (the default is 10 minutes) to ensure that the upgrade is successful. If you enable the auto-commit option, the system automatically commits to the new software version after the commit timer expires. If you disable the auto-commit option, you must issue the software commit command before the commit timer expires to commit the new software version, otherwise the system restarts automatically to the previous (committed) version. By default, auto-commit is enabled.

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. **(Optional)** Configure the timer to activate the software:

   `sys software commit-time <10-60>`

   The default is 10 minutes.

3. **(Optional)** Extend or reduce the time to commit the software:

   software reset-commit-time [<1–60>]

4. Commit the upgrade:

   ```
   software commit
   ```

Downgrading the software

Perform this procedure to downgrade the switch from the current trusted version to a previous release.

Important:

In VOSS 4.2 and later, the encryption modules are included in the image file. Therefore, the **`load-encryption`** command and the **`software add-module`** command is present but no longer applicable to the current release. You do not require an ACLI command to add or load the encryption module. Use the **`software add-module`** command only if you downgrade to a release earlier than VOSS 4.2.

Before you begin

Ensure that you have a previous version installed.

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]
   ```

   Note:

   This step applies to downgrades to a software version earlier than VOSS 4.2.

4. Activate a prior version of the software:

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

5. Restart the switch:

   ```
   reset
   ```

   Important:

   After you restart the system, you have the amount of time configured for the commit timer to verify the software change 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 expires. This feature ensures you can regain control of the system if an upgrade fails. By default, auto-commit is enabled.

6. Commit the software change:

   ```
   software commit
   ```

   Important:

   If you do not enable the auto-commit functionality, you must commit the software change before the commit timer expires. This is an optional step otherwise.

7. Verify the downgrade:

   - Check for alarms or unexpected errors using the `show logging file tail` command.
   - Verify all modules and slots are online using the `show sys-info` command.

8. **(Optional)** Remove unused software:

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

Variable definitions

Use the data in the following table to use the `software` command.

Variable	Value
activate WORD<1-99>	Specifies the name of the software release image.
add WORD<1-99>	Specifies the path and version of the compressed software release archive file.
remove WORD<1-99>	Specifies the path and version of the compressed software release archive file.

Deleting a software release

Perform this procedure to remove a software release from the switch.

Note:

There is a limit of six software releases that can be stored on the switch. If you have six releases already stored on the switch, then you will be prompted to remove one release before you can proceed with adding and activating a new software release.

Procedure

1. Enter Privileged EXEC configuration mode:

   ```
   enable
   ```

2. Remove software:

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

Example

The following example is for the VSP 4000 switch, but the same steps apply to other VOSS switches.

```
VSP-4450GSX-PWR+:1>enable

VSP-4450GSX-PWR+:1#software remove VSP4K.4.1.0.0
```

Upgrading the boot loader image

Warning:

This command is an advanced-level command that upgrades the device uboot image. Only use this command if specifically advised to do so by Avaya Support. Improper use of this command can result in permanent damage to the device and render it unusable.

If the need to use this command arises, instructions on usage will be provided by Avaya Support.

Before you begin

- Transfer the image to the `/intflash/` directory on the switch.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the current uboot version:

   ```
   show sys-info uboot
   ```

3. Upgrade the boot loader image:

   ```
   uboot-install WORD<1-99>
   ```

Variable definitions

Use the data in the following table to use the **`uboot-install`** command.

Variable	Value
WORD<1-99>	Specifies the full path and filename that contains the uboot image.

Chapter 5: Known issues and limitations

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

Known issues in this release

This section identifies the known issues in this release for the following products:

- VSP 4000 Series
- VSP 7200 Series
- VSP 8000 Series

Device related issues

Table 23: Known issues

Issue number	Description	Workaround
wi01144867	On the port that is removed from a T-UNI LACP MLT, non T-UNI configuration is blocked as a result of T-UNI consistency checks.	When a port is removed from a T-UNI LACP MLT, the LACP key of the port must be set to `default`.
wi01166763	SLA Mon™ tests fail (between 2% and 8% failure) between VSP 4000 devices when you have too many agents involved with scaled configurations.	This happens only in a scaled scenario with more than seven agents, otherwise the failure does not occur. The acceptable failure percentage is 5%, but you may see failures of up to 8%.
wi01168610	VSP 4450GSX: The command **sys shutdown** does not change the STATUS LED on the VSP 4450GSX-PWR+ device.	None. This issue does not impact any functionality.
wi01168706	The following error message occurs on VSP 4000 when performing **shutdown/no-shutdown** commands continuously: `IO1  [05/02/14 06:59:55.178:UTC] 0x0011c525 00000000 GlobalRouter COP-SW ERROR vsp4kTxEnable Error`	None. When this issue occurs, the port in question may go down, then performs a **shutdown/no-shutdown** of the port to bring it up and resumes operation.

Table continues…

Issue number	Description	Workaround
	`changing TX disable for SFP module: 24, code: -8`	
wi01171802	VSP 4450GSX: On a fresh boot, peer ports connected to ports 1/49 and 1/50 bounce and may cause additional transitions in the network.	None.
wi01171907	VSP 4450GSX: CAKs are not cleared after setting VSP 4000 to factory-default.	None. Currently this is the default behavior and does not affect functionality of the MACsec feature.
wi01173026	A reboot with verbose configuration does not allow you to delete a VRF.	This issue occurs only if you save the configuration file in verbose mode and reboot the switch in that configuration. This situation is unlikely to exist; verbose mode is used more as a diagnostic tool. This issue does not impact functionality.
wi01173136	T1 SFP: Shutting down the T1 link from one end of the VSP 4000 or VSP 7200 Series or VSP 8000 Series does not shut down the link at the remote end. You may experience traffic loss if the remote side of the link is not shut down.	This issue occurs only when a T1 SFP link from one end is shutdown. Enable a dynamic link layer protocol such as LACP or VLACP on both ends to shut the remote end down too. As an alternative, administratively disable both ends of the T1 SFP link to avoid the impact.
wi01175118	On a MACsec enabled port, you may see delayed packets when the MACsec port is kept running for more than 12 hours. This delayed packet counter may also increment when there is complete reordering of packets so that the application might receive a slow response. But in this second case, it is a marginal increase in the packet count, which occurs due to PN mismatch sometimes only during Key expiry, and does not induce any latency.	None.
wi01195988	You cannot use EDM to issue ping or traceroute commands for IPv6 addresses.	Use ACLI to initiate ping and traceroute.
wi01196000	You cannot use EDM to issue ping or traceroute commands for IPv4 addresses.	Use ACLI to initiate ping and traceroute.
wi01197712	On the 40-gigabit ports, the small metallic fingers that surround the ports are fragile and can bend out of shape during removal and insertion of the transceivers. When the fingers are bent, they prevent the insertion of the QSFP+ transceiver.	Insert the QSFP+ carefully. If the port gets damaged, it needs to be repaired.

Table continues…

Issue number	Description	Workaround
	Note: This issue is specific to VSP8404QQ ESMs.	
wi01207076	If you configure both IPv4 and IPv6 on a VLAN interface, and then change the IPv6 MTU, the IPv4 MTU is also changed for that interface.	Configure a MTU value, up to 9500 bytes, that is higher than the default. The default MTU for an IPv6-enabled VLAN is 1500 bytes.
wi01208650	The Console gets disconnected frequently when you enable screen trace (trace screen enable). The error displayed is `Forced log-out after 65535 secs`.	None
wi01209346	In an 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. • The Indiscard packet count gets incremented on the **`show int gig error`** statistics command.	Use a v3 interface as querier in a LAN segment which has snoop– enabled v2 and v3 interfaces.
wi01209604	From EDM, you cannot perform a Layer 2 IP PING for an IPv6 address. EDM displays the following error: `No next Hop address found for ip address provided`.	Use the ACLI perform a Layer 2 IP PING.
wi01210104	In EDM, you cannot select multiple 40–gigabit ports or a range of ports that includes 40–gigabit ports to graph or edit. You need to select them and edit them individually. **Note:** This issue applies to products that support 40 Gbps ports.	None.
wi01212099	In the COM EDM Plugin command, the Layer 2 Traceroute IPv6 does not work properly and gives the error, `No Such Name`.	Use the ACLI to initiate the Layer 2 Traceroute for IPv6.
wi01212115	On EDM, the port LED for channelized ports only shows the status of sub-port #1, but not the rest of the sub-ports. When you remove sub-port #1, and at least one other sub-port is active and online, the LED color changes to amber, when it should be green because at	None.

Table continues…

Issue number	Description	Workaround
	least one other sub-ports is active and online. The LED only shows the status of sub-port #1.	
wi01212860	An intermittent link-flap issue can occur in the following circumstance for the copper ports of the VSP 7254XTQ or the 8424XT ESM for VSP 8400: If you use a crossover cable and disable auto-negotiation, the port operates at 100 Mbps. A link flap issue can occur intermittently and link flap detect will shutdown the port.	Administratively shutdown, and then reenable the port. **Note:** Avaya recommends that you use auto-negotiation. Disabling auto-negotiation on these ports is not a recommended configuration.
wi01214025	Traffic is forwarded to IGMP v2 SSM group, even after you delete the IGMP SSM-map entry for the group.	If you perform the delete action first, you can recreate the SSM-map record, and then disable the SSM-map record. The disabled SSM-map record causes the receiver to timeout because any subsequent membership reports that arrive and match the disabled SSM-map record are dropped. You can delete the SSM-map record after the receivers time out.
wi01214772	The 4 byte AS confederation identifier and peers configuration are not retained across a reboot. This problem occurs when 4 Byte AS is enabled with confederation.	Reconfigure the 4 byte AS confederation identifier and peers on the device, and reboot.
wi01215220	After you enable enhanced secure mode, and log in for the first time, the system prompts you to enter a new password. If you do not meet the minimum password requirements, the following system output message appears: `Password should contain a minimum of 2 upper and lowercase letters, 2 numbers and 2 special characters like !@#$%^*(). Password change aborted. Enter the New password:` The system output message does not display the actual minimum password requirements you need to meet, which are configured on your system. The output message is an example of what the requirements may need to meet. The actual minimum password requirements you need to meet are configured on your system by the administrator.	None.
wi01215773	The switch provides an NTP log message that indicates that the NTP server did not synchronize, even though one of the NTP	None.

Table continues…

Issue number	Description	Workaround
	servers synchronized correctly and the NTP stats show that it did.	
wi01216535	The `router ospf` entry always appears in the configuration file regardless of whether OSPF is configured. This line does not perform any configuration and has no impact on the running software.	None.
wi01216550	When you use Telnet or SSH to connect to the switch, it can take up to 60 seconds for the login prompt to appear. However, this situation is very unlikely to happen, and it does not appear in a standard normal operational network.	Do not provision DNS servers on a switch to avoid this issue altogether.
wi01217251	If you configure egress mirroring on NNI ports, you do not see the MAC-in-MAC header on captured packets.	Use an Rx mirror on the other end of the link to see the packets.
wi01217347	A large number of IPv6 VRRP VR instances on the same VLAN can cause high CPU utilization.	Do not create more than 10 IPv6 VRRP VRs on a single VLAN.
wi01217871	If you attach the QSFP+ end of a passive breakout cable to a VSP 4000 or VSP 7200 Series or VSP 8000 Series switch, and the SFP+ ends of the cable to a VSP 9000 running Release 4.0.1, the output for the **`show pluggable-optical-modules basic`** command on the VSP 9000 shows an incorrect vendor name and part number. The incorrect information also appears in EDM under the **Edit** > **Port** > **General** menu path.	This issue will be fixed in a future VSP 9000 software release.
wi01218707 / VOSS-1374	If you use a passive copper breakout cable between a channelized 40 Gbps port on a VSP 8400 and a 10 Gbps port on a 9024XL module in a VSP 9000, the link can occasionally drop. VSP 9000 9024XL I/O modules do not support the following breakout cables: • QSFP+ to 4 SFP+ breakout cable, 1 meter (Passive), AA1404033-E6 • QSFP+ to 4 SFP+ breakout cable, 3 meter (Passive), AA1404035-E6 • QSFP+ to 4 SFP+ breakout cable, 5 meter (Passive), AA1404036-E6	For alternate use on the 9024XL I/O module, you can use a 40GBASE-SR4 QSFP+ transceiver on the distant channelized 40 GigabitEthernet interface, with a fiber breakout patch lead connecting into 4 x 10GBASE-SR/SW SFP+ (AA1403015-E6) transceivers used in the 9024XL ports.

Table continues…

Issue number	Description	Workaround
wi01221817	If you disable IPv6 on one RSMLT peer, the switch can intermittently display `COP-SW ERROR` and `RCIP6 ERROR` error messages. This issue has no impact.	None.
wi01222078	If you delete the SPBM configuration and re-configure SPBM using the same nickname but a different ISIS system id without rebooting, the switch displays an error message.	Reboot the switch after you delete the SPBM configuration.
wi01223719	You cannot use EDM to configure SSH rekey and enable or disable SFTP.	Use ACLI to configure SSH rekey and enable or disable SFTP.
wi01223723	EDM displays the user name as Admin, even though you login using a different user name.	None.
wi01223759	You cannot use EDM to view the IPv6 DHCP relay counters.	Use ACLI to view the IPv6 DHCP relay counters.
wi01224076	When you re-enable insecure protocols in the ACLI SSH secure mode, the switch does not display a warning message.	None.
wi01224644	EDM displays the IGMP group entry that is learnt on vIST MLT port is as TX-NNI.	Use ACLI to view the IGMP group entry learnt on vIST MLT port.
wi01224710	On a VSP 4000 Series untagged ARP packet, ingressing on a Layer 2 VSN interface will honor default the port QOS. Changing port QOS value will not be honored.	Create an ACLI filter that can remark the packet to any Queues .
wi01225023	When port-lock is enabled on the port and re-authentication on the EAP client fails, the port is removed from the radius assigned VLAN. This adds the port to default VLAN and displays an error message. This issue has no impact.	The error message is incorrect and can be ignored.
wi01225232	When an operational SMLT is removed from a TUNI ISID and is not added to any other VLAN or TUNI ISID, then spanning tree is enabled on this SMLT interface. Spanning tree is disabled when added to VLAN or TUNI ISID. This issue has no impact.	Disable SMLT ports and then remove them from TUNI ISID.
wi01225310	When ISIS is disabled on one of the VIST peer nodes with RSMLT interfaces and it has ECMP routes with the RSMLT Peer as the next hop, the ECMP routes that are being replaced during the transition of the ISIS state now will have a next hop of the local interface. This results in an error message `COP-SW`	Enable ISIS on both the vIST peers.

Table continues…

Issue number	Description	Workaround
	`ERROR ercdProcIpRecMsg: Failed to Replace IP Records`.	
wi01225514	On a VSP 7200 Series 40 Gbps ports with CR4 direct attach cables (DAC), when you manually enable or disable ISIS, the port bounces once.	Configure ISIS during the maintenance period. Bring the port down, configure the port and then bring the port up.
wi01226335	In a rare scenario in Simplified vIST configuration when vIST state is toggled immediately followed by vIST MLT ports are toggled, one of the MLT ports will go into blocking state resulting in failure to process data packets hashing to that link.	Before enabling vIST state ensure all VIST MLT ports are shut and re-enabled after vIST is enabled on the DUT.
wi01226433 wi01226437	When you configure a scaled Layer 3 VSN (24 Layer 3 VSN instances), route leaking from GRT to VRF on the local DUT does not happen. The switch displays an incorrect error message `Only 24 L3 VSNs can be configured`.	None.
wi01227920 wi01230534	The packet internal CoS is derived incorrectly for packets sourced from a brouter port when the CoS should be derived from the port level QoS. The following list identifies scenarios that derive the internal CoS from the port QoS: • Untagged non-IP packet • Untagged IP packet, and the source port is Layer 3 untrusted • Tagged non-IP packet and the source port is Layer 2 untrusted • Tagged IP packet and the source port is Layer 3 untrusted and Layer 2 untrusted.	Use the port default QoS configuration for the brouter port. The port default configuration is Layer 2 trusted and Layer 3 trusted, and under this configuration, only the first scenario in the list is still an issue. The other scenarios do not occur.
wi01230533 wi01230953 wi01232817	When you use Fabric Extend over IP (FE-IP) and Fabric Extend over L2 VLAN (FE-VID) solution, if you change the ingress and egress .1p map, packets may not follow correct internal QoS queues for FE tunnel to FE tunnel, or FE tunnel to regular NNI traffic. .	Do not change the default ingress and egress .1p maps when using Fabric Extend. With default ingress and egress . 1p maps, packets follow the correct internal QoS when using the Fabric Extend feature
wi01232095	EDM and ACLI show different local preference values for a BGP IPv6 route. EDM displays path attributes as received and stored in the BGP subsystem. If the attribute is from an eBGP peer, the local preference appears as zero.	None

Table continues…

Issue number	Description	Workaround
	ACLI displays path attributes associated with the route entry, which can be modified by a policy. If a route policy is not configured, the local preference shows the default value of 100.	
wi01232581	You cannot use EDM to enable or disable ASG. You can only view ASG status.	Use ACLI to enable or disable ASG.
wi01233201	If the I-SID associated with a Switched UNI or Fabric Attach port does not have a platform VLAN association and you disable Layer 2 Trusted, then the non IP traffic coming from that port does not take the port QoS and still uses the .1p priority in the packet.	None
wi01233828	If you establish an SSH connection to a switch, and then use that switch to create a Telnet session with another device, when you exit the Telnet session, the original SSH connection can stop responding.	Halt the original SSH connection and reconnect.
wi01234422	If you improperly close an SSH session, the session structure information does not clear and the client can stop functioning.	Disable and enable SSH.
wi01234071	You cannot use EDM to clear Fabric Attach statistics for VSP 4000 Series.	Use the ACLI **`clear fa stats`** command.
wi01234623	VSP 7200 Series and VSP 8000 Series do not Support Fabric Extend over Layer 2 VLAN (FE-VID) logical interface configuration over an MLT interface.	None
wi01234739	If you apply an ipv6-out-route-map on a BGP peer to filter a particular IPv6 prefix range with a match network condition, it does not filter the full prefix range.	Configure the incoming policy to filter incoming advertised routes on BGP+ peers.
wi01234872	The **`show debug-file all`** command is missing on VSP 7200 Series and VSP 8000 Series platforms.	None
wi01234873	The system does not generate a log message, either in the log file or on screen, when you run the **`flight-recorder`** command.	None
wi01235018	If you use an ERS 4850 FA Proxy with a VOSS FA Server, a mismatch can exist in the show output for tagged management traffic. The ERS device always sends traffic as tagged. The VOSS FA Server can send both tagged and untagged. For untagged, the VOSS FA Server sends VLAN ID 4095 in the	There is no functional impact.

Table continues…

Issue number	Description	Workaround
	management VLAN field of the FA element TLV. The ERS device does not recognize this VLAN ID and so still reports the traffic as tagged.	
wi01235053	If you use EDM to create an ACL filter, the ACL tab does not automatically refresh to show the new filter.	Click **Refresh** on the ACL tab to force a data refresh.
wi01235138	When a new VRF is created, the system associates all community string entries that belong to the GRT context with the VRF ID for VRF management. An incorrect community string is created for this new VRF if configuration flow is as follows: create a new SNMP community with a community entry INDEX that is lower than existing entries with the length of the community string longer than existing entries, followed by the addition of a new VRF.	When you create a new community string: • If the length of the new string is longer than the existing community string, use an INDEX that is greater than the INDEX of the existing entry. • If the length of the new string is shorter than the existing community string, use an INDEX that is lower than the INDEX of the existing entry. If the configuration steps resulted in an incorrect string being created for a new VRF, then delete the higher INDEX communities and recreate them.

wi01235140	You cannot configure an untagged-traffic ELAN endpoint and enable BPDU in the same command.	1. Create the untagged-traffic endpoint first:
		`untagged-traffic port {slot/port[/sub-port][-slot/port[/sub-port]][,...]`
		OR
		`untagged-traffic mlt <1-512>`
		2. Enable BPDU:
		`untagged-traffic port {slot/port[/sub-port][-slot/port[/sub-port]][,...] bpdu enable`
		OR
		`untagged-traffic mlt <1-512> bpdu enable`

wi01235322	Secure Copy (SCP) file transfers on VSP switches, running VOSS 5.0, stall intermittently due to 100% thread utilization of the SCP process, which is responsible for file transfer. This problem is seen intermittently	In the event of a stalled file transfer session, you can exit gracefully by closing the SCP client using **Ctrl** + **c**, or by disabling, and then re-enabling the

Table continues…

Issue number	Description	Workaround
	when the transfer is initiated from SSH client versions earlier than OpenSSH_5.0, or for files with size of 1 GB or larger. For client versions later than OpenSSH_5.0, this stall condition is rare for file sizes up to 500 MB and has not been seen for files with sizes that are typically transferred to and from VOSS switches. The use of some older client versions such as the ones shown in the following list always result in stalled file transfers: • Sun_SSH_1.1, SSH protocols 1.5/2.0, OpenSSL 0x0090704f • OpenSSH_3.9p1, OpenSSL 0.9.7a Feb 19 2003 The recommended client and file size range to avoid this problem is to use Open SSH client version later than 5.0 and file sizes up to 500 MB.	SSH server on the switch, which clears all open sessions.
VOSS-1747	On a VSP 8404 with MLT on 10G ports on an 8424XT or 8424XTQ module, multiple VLANs that have the MLT as a member of the VLAN, there is a possibility that a copy of the IP multicast traffic may not be sent on all VLANs that have a receiver on the MLT.	None
VOSS-1757	Configuration of Fabric Attach requires RWA access to the switch.	None
VOSS-1758	After changing ISIS System-ID, it is possible that CFM L2 ping will not work properly.	Utilize L2traceroute command (provides all hops along the path rather than a specific hop only).

Limitations in this release

This section lists known limitations and expected behaviors that may first appear to be issues.

Limitations for VSP 4450GTX-HT-PWR+

⚠ **Caution:**

The VSP 4450GTX-HT-PWR+ has operating temperature and power limitations. For safety and optimal operation of the device, ensure that the prescribed thresholds are strictly adhered to.

The following table provides a description of the limitation or behavior and the work around, if one exists.

Table 24: Limitations for VSP 4450GTX-HT-PWR+

Behavior	Description	Workaround
For high-temperature threshold	The VSP 4450GTX-HT-PWR + supports a temperature range of 0°C to 70°C. In the alpha release, power supply does not shut down at an intended over-temperature threshold of 79°C.	To prevent equipment damage, ensure that the operating temperature is within the supported temperature range of 0°C to 70°C.
For power supply wattage threshold	Software functionality to reduce the POE power budget based on the number of operational power supplies and operating temperature is not available in the Alpha SW image.	Ensure that the POE device power draw is maintained at the following when the device is at temperatures between 61°C and 70°C: • 400W — with 1 operational power supply • 832W — with 2 operational power supplies
For inoperable external USB receptacle	The VSP 4450GTX-HT-PWR+ has an empty external USB receptacle that was not available in GTS models. Software to support the use of the external USB receptacle is not yet available in the Alpha SW image. Therefore the USB port is inoperable.	No workarounds are provided with the alpha image.

General limitations and expected behaviors

The following table provides a description of the limitation or behavior.

Table 25: General limitations and expected behaviors

WI number	Description
wi01068569	The system displays a warning message that routes will not inject until the apply command is issued after the enable command. The warning applies only after you enable redistribution, and not after you disable redistribution. For example, `4k2:1(config)#isis apply redistribute direct vrf 2`.
wi01112491	IS-IS enabled ports cannot be added to an MLT. The current release does not support this configuration.
wi01122478	Stale SNMP server community entries for different VRFs appear after reboot with no VRFs .

Table continues…

WI number	Description
	On a node with a valid configuration file saved with more than the default vrf0 , SNMP community entries for that VRF are created and maintained in a separate text file, snmp_comm.txt, on every boot. The node reads this file and updates the SNMP communities available on the node. As a result, if you boot a configuration that has no VRFs, you may still see SNMP community entries for VRFs other than the globalRouter vrf0 .
wi01137195	A static multicast group cannot be configured on a Layer 2 VLAN before enabling IGMP snooping on the VLAN. After IGMP snooping is enabled on the Layer 2 VLAN for the first time, static multicast group configuration is allowed, even when IGMP snooping is disabled later on that Layer 2 VLAN.
wi01138851	Configuring and retrieving licenses using EDM is not supported.
wi01141638	On a VSP 4000, when a VLAN with 1000 multicast senders is deleted, the console or Telnet session stops responding and SNMP requests time out for up to 2 minutes.
wi01142142	When a multicast sender moves from one port to another within the same BEB or from one VIST peer BEB to another, with the old port operationally up, the source port information in the output of the **`show ip igmp sender`** command is not updated with new sender port information. You can perform one of the following workarounds: • On an IGMP snoop-enabled interface, you can flush IGMP sender records. ⚠ **Caution:** Flushing sender records can cause a transient traffic loss. • On an IGMP-enabled Layer 3 interface, you can toggle the IGMP state. ⚠ **Caution:** Expect traffic loss until IGMP records are built after toggling the IGMP state.
wi01145099	IP multicast packets with a time-to-live (TTL) equal to 1 are not switched across the SPB cloud over a Layer 2 VSN. They are dropped by the ingress BEB. To prevent IP multicast packets from being dropped, configure multicast senders to send traffic with TTL greather than 1.
wi01159075	**VSP 4450GSX-PWR+**: Mirroring functionality is not working for RSTP BPDUs.
wi01171670	Telnet packets get encrypted on MACsec enabled ports.
wi01198872	On a VSP 4000, loss of learned MAC addresses occurs in a vIST setup beyond 10k addresses. In a SPB setup the MAC learning is limited to 13k MAC addresses, due to the limitation of the internal architecture when using SPB. Moreover, as vIST uses SPB and due to the way vIST synchronizes MAC adresses with a vIST pair, the MAC learning in a vIST setup is limited to 10K Mac addresses.
wi01210217	The command **`show eapol auth-stats`** displays LAST-SRC-MAC for NEAP sessions incorrectly.

Table continues…

WI number	Description
wi01211415	In addition to the fan modules, each power supply also has a fan. The power supply stops working if a power supply fan fails, but there is no LED or software warning that indicates this failure. Try to recover the power supply fan by resetting the switch. If the fan does not recover, then replace the faulty power supply.
wi01212034	When you disable EAPoL globally: • Traffic is allowed for static MAC configured on EAPoL enabled port without authentication. • Static MAC config added for authenticated NEAP client is lost.
wi01212247	BGP tends to have many routes. Frequent additions or deletions impacts network connectivity. To prevent frequent additions or deletions, reflected routes are not withdrawn from client 2 even though they are withdrawn from client 1. Disabling Route-reflection can create blackhole in the network. Workaround: Bounce the BGP protocol globally.
wi01212585	LED blinking in EDM is representative of, but not identical to, the actual LED blinking rates on the switch.
wi01213040	When you disable auto-negotiation on both sides, the 10 Gbps copper link does not come up.
wi01213066 wi01213374	EAP and NEAP are not supported on brouter ports.
wi01213336	When you configure `tx` mode port mirroring on T-UNI and SPBM NNI ports, unknown unicast, broadcast and multicast traffic packets that ingress these ports appear on the mirror destination port, although they do not egress the mirror source port. This is because `tx` mode port mirroring happens on the mirror source port *before* the source port squelching logic drops the packets at the egress port.
wi01219295	SPBM QOS: Egress UNI port does not follow port QOS with ingress NNI port & Mac-in-Mac incoming packets.
wi01219658	The command **`Show khi port-statistics`** does not display the count for NNI ingress control packets going to the CP.
wi01223526	ISIS logs duplicate system ID only when the device is a direct neighbor.
wi01223557	Multicast outage occurs on LACP MLT when simplified vIST peer is rebooted. You can perform one of the following work arounds: • Enable PIM on the edge. • Ensure that IST peers are either RP or DR but not both.
wi01224683 wi01224689	Additional link bounce may occur on the following ports, when toggling links or during cable re-insertion: • VSP 7254XSQ 10 Gbps port • VSP 7254XSQ and VSP7254XTQ 40Gig optical cables and 40 Gbps break out cables

Table continues…

WI number	Description
	• VSP 8200 and VSP 8400 40 Gbps ports with optical cable • VSP 8200 and VSP 8400 40 Gbps ports with optical breakout cable
wi01229417	Origination and termination of IPv6 6-in-4 tunnel is not supported on a node with vIST enabled.
wi01232578	When SSH keyboard-interactive-auth mode is enabled, the server generates the password prompt to be displayed and sends it to the SSH client. The server always sends an expanded format of the IPv6 address. When SSH keyboard-interactive-auth mode is disabled and password-auth is enabled, the client itself generates the password prompt, and it displays the IPv6 address format used in the `ssh` command.
wi01234289	HTTP management of the ONA is not supported when it is deployed with a VSP 4000 Series device.

SSH connections

VOSS 4.1.0.0 and VOSS 4.2.0.0 SSH server and SSH client support password authentication mode.

VOSS 4.2.1.0 changed the SSH server from password authentication to keyboard-interactive. VOSS 4.2.1.0 changed the SSH client to automatically support either password authentication or keyboard-interactive mode.

In VOSS 4.2.1.0, you cannot configure the SSH server to support password authentication. This limitation creates a backward compatibility issue for SSH clients that do not support keyboard-interactive mode, including SSH clients that are part of pre-VOSS 4.2.1.0 software releases. For example, VOSS 4.1.0.0 SSH clients, VOSS 4.2.0.0 SSH clients, and external SSH clients that only support password authentication cannot connect to VOSS 4.2.1.0 SSH servers.

This issue is addressed in software release VOSS 4.2.1.1 and later. The default mode of the SSH server starting from VOSS 4.2.1.1 is changed back to password authentication. Beginning with VOSS 5.0, you can use an ACLI command to change the SSH server mode to keyboard-interactive. For more information about how to configure the SSH server authentication mode, see *Administration for Avaya Virtual Services Platform 4000 Series*, NN46251-600 or *Administering Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-600.

Note:

If you enable the ASG feature, the SSH server must use keyboard-interactive.

See the following table to understand SSH connections between specific client and server software releases.

Client software release	Server software release	Support
VOSS 4.1.0.0	VOSS 4.2.0.0	Supported
VOSS 4.1.0.0	VOSS 4.2.1.0	Not supported
VOSS 4.2.0.0	VOSS 4.2.1.0	Not supported
VOSS 4.1.0.0	VOSS 4.2.1.1	Supported
VOSS 4.2.0.0	VOSS 4.2.1.1	Supported

Chapter 6: Resolved issues

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

Fixes from previous releases

VOSS 5.0 incorporates all fixes from prior releases, up to and including VOSS 4.2.2.0.

Table 26: Resolved issues in this release

WI reference	Description
wi01174787	Using EDM, you cannot create static ARP entries. This issue was resolved in this release.
wi01212591	IPv4 shortcut traffic is going to queue 0 on the non-gateway device of the vIST pair. The packet can be en-queued incorrectly, so if the queue is congested, the packet maybe unexpectedly dropped. If such a packet causes queue congestion, then the incorrect queue would be congested. Note that this WI is specific to the VSP 4000. This issue was resolved in this release.
wi01221371	On a 10 Gbps port when auto–negotiation is enabled on an operational MLT port and then the second link is made operational, the first MLT link goes into blocking state. This results in traffic loss for all the traffic hashing to the blocked link. This issue was resolved in this release.
wi01221497	In rare cases when you enable or disable the E-Tree promiscuous or isolated port, MAC address learned for vIST peers will not be displayed in the MAC table. This issue was resolved in this release.
wi01225045	When multiple ports exist in an MLT and user configures rate-limiting on any one of the ports, the configuration is applied to all MLT members. When a new port is added into the MLT, the rate-limiting configuration of the MLT ports is not applied to the newly added port. It keeps its own rate limiting properties. This issue was resolved in this release.
wi01226215	On a VSP 7254XSQ when you swap an existing 1 Gbps Copper SFP with another type of SFP the link does not come up. This issue was resolved in this release.
wi01227818	Low temperature alarms can appear for 40GBASE-LM4 QSFP+ transceivers if you enable DDM monitoring:

Table continues…

WI reference	Description

	`CP1 [07/02/15 12:26:18.576:UTC] 0x00004686 00000000 GlobalRouter SNMP WARNING Temperature Low Alarm (1/41)`
	`CP1 [07/02/15 12:26:25.016:UTC] 0x00004686 00000000 GlobalRouter SNMP WARNING Temperature Normal (1/41)`
	These messages have no functional impact. The low temperature alarm is cleared in the next DDM monitoring interval.
	This issue was resolved in this release.