Release Notes for Avaya Virtual Services Platform 7000 Series

Release 10.4
NN4702-400
Issue 10.07
February 2016

© 2014-2016, Avaya, Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

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

License types

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

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You a license to use Heritage Nortel

Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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.

Note to Service Provider

The product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose

This document provides overview information about the new features supported in this software release for the Avaya Virtual Services Platform 7000 Series.

Related resources

Documentation

For a list of the documentation for this product, see *Documentation Roadmap Reference for Avaya Virtual Services Platform 7000 Series*, NN47202–103.

Training

Ongoing product training is available. For more information or to register, see http://avaya-learning.com/.

Enter the course code in the **Search** field and click **Go** to search for the course.

Course code	Course title
7D00080W	Avaya Stackable ERS and VSP Product Overview
7D00085V	Stackable ERS & VSP Installation, Configuration, and Maintenance
7D00085I	Stackable ERS & VSP Installation, Configuration, and Maintenance

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.

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.

Subscribing to e-notifications

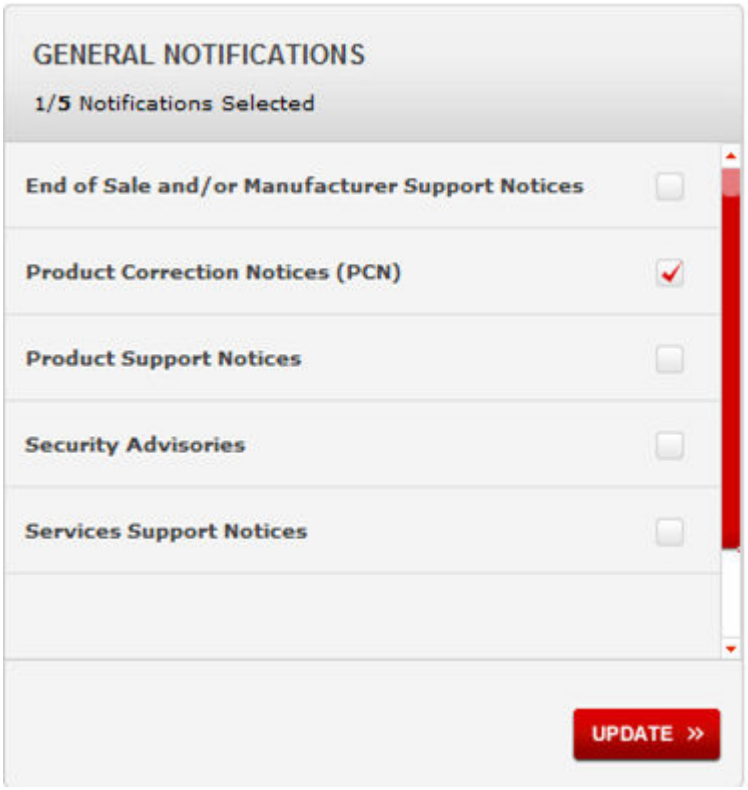
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

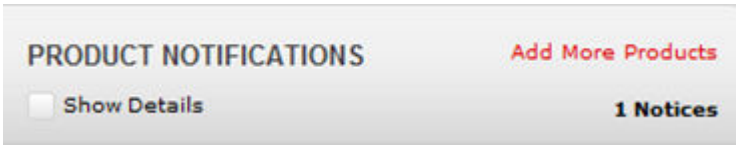
You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Ethernet Routing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

Procedure

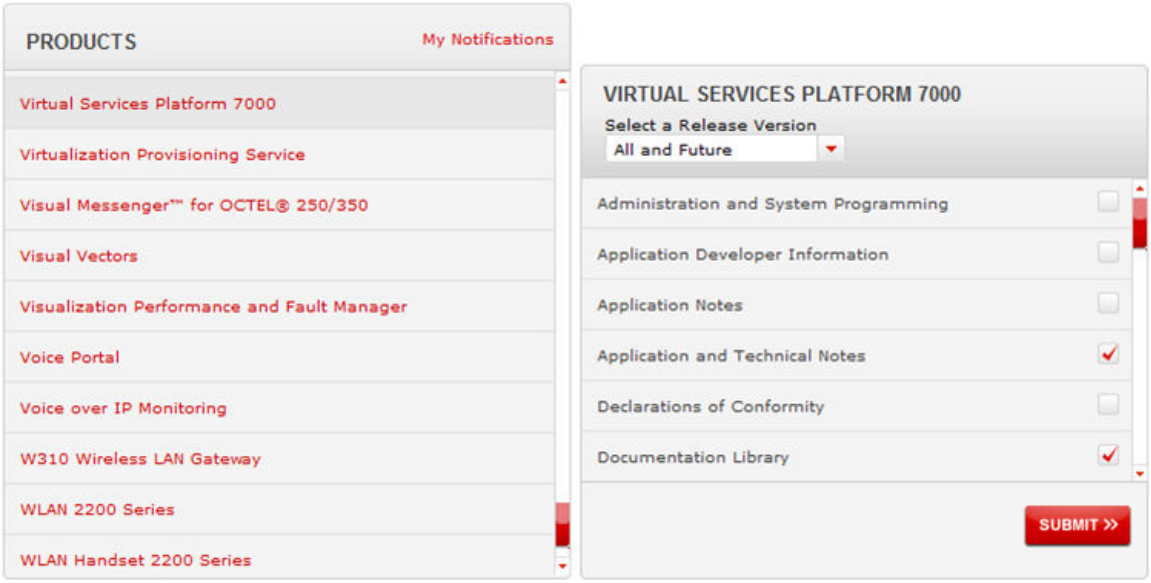
1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click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



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



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



11. Click **Submit**.

Chapter 2: New in this release

The following sections detail what is new in this document for VSP 7000 Release 10.4.

Features

See the following sections for information about feature changes.

40GE Full MD5 authentication

The QSFP+ transeivers operates in strict mode. When a new QSFP + module is detected, the PEC code is validated and for qualified QSFP + modules, password authentication is performed.

For more information, see *Installing Transceivers and Optical Components on Avaya Virtual Services Platform 7000 Series*, NN47202–302.

BPDU filtering on trunk

The BPDU filtering on trunk feature provides loop protection on ports that belong to MLT, DMLT, or LAC trunks.

When BPDU filtering state or timeout of a port is configured, the BPDU filtering on trunk checks if the port belongs to an MLT, DMLT, or LAC trunk, in which case the settings are propagated to all ports from that trunk.

For more information, see *Configuring Layer 2 on Avaya Virtual Services Platform 7000 Series*, NN47202–502.

Fabric Attach

Fabric Attach (FA) extends the fabric edge to devices that do not support Shortest Path Bridging MAC (SPBM). With FA, non-SPBM devices can take advantage of full SPBM support, when support is available.

FA also decreases the configuration requirements on SPBM devices by off-loading some configuration to the attached non-SPBM devices and by automating certain configuration steps that occur most often.

FA Proxy Standalone or FA Proxy and SPB are mutually exclusive features on VSP 7000. For VSP 7000 deployments that have SPB enabled, you cannot enable FA Proxy or FA Standalone Proxy functionality.

In Release 10.4, the FA feature provides the following enhancements:

- C-VLAN join support
- Auto provision support
- Zero-touch support
- Standalone FA Proxy
- Fabric Attach Proxy

For more information about the FA feature, see *Configuring Avaya Fabric Connect on Avaya Virtual Services Platform 7000 Series*, NN47202–510.

ACLI commands

This feature introduces the following ACLI commands:

- fa authentication-key
- default fa authentication-key
- fa message-authentication
- default fa message-authentication
- no fa message-authentication
- fa extended-logging
- no fa extended-logging
- fa port-enable
- default fa port-enable
- no fa port-enable
- fa proxy
- default fa proxy
- no fa proxy
- fa standalone-proxy
- default fa standalone-proxy
- no fa standalone-proxy
- fa timeout
- default fa timeout
- fa uplink

- no fa uplink
- fa vlan
- no fa vlan
- fa zero-touch
- no fa zero-touch
- default fa zero-touch
- fa zero-touch-options
- no fa zero-touch-options
- default fa zero-touch-options
- show fa agent
- show fa elements
- show fa i-sid
- show fa port-enable
- show fa uplink
- show fa vlan
- show fa zero-touch-options

For more information about ACLI commands, see *ACLI Commands Reference for Avaya Virtual Services Platform 7000 Series*, NN47202–600.

IGMP enhancements

Unknown multicast filtering

IGMP unknown multicast filtering is no longer supported on the Avaya Virtual Services Platform 7000 Series starting with the 10.4.0 release. The functionality provided by this feature has been integrated with IGMP Snooping. When IGMP Snooping is activated on a vlan, unknown multicast traffic is no longer flooded on all vlan ports but it is forwarded only on mrouter ports.

For more information, see *Configuring IP Routing on Avaya Virtual Services Platform 7000 Series*, NN47202–511.

Multicast filter mode

In Release 10.4, Multicast filter mode functionality is not supported.

ACLI commands not supported

The following ACLI commands are not supported in Release 10.4:

- vlan igmp unknown-mcast-no-flood
- default vlan igmp unknown-mcast-no-flood
- vlan igmp unknown-mcast-allow-flood
- no vlan igmp unknown-mcast-allow-flood

- default vlan igmp unknown-mcast-allow-flood
- show vlan igmp unknown-mcast-no-flood
- show vlan igmp unknown-mcast-allow-flood
- show ip igmp multicast-filter-mode
- ip igmp multicast-filter-mode
- no ip igmp multicast-filter-mode
- default ip igmp multicast-filter-mode

IPv6 host mode enhancement

IPv6 host mode enhancement is an extension of the IPv6 management application, which supports several settings that are not available by default on the in-band/out-of-band management interface.

For more information, see *Configuring Layer 2 on Avaya Virtual Services Platform 7000 Series*, NN47202–502, *Getting Started with Avaya Virtual Services Platform 7000 Series*, NN47202–303, and *Configuring IP Routing on Avaya Virtual Services Platform 7000 Series*, NN47202–511.

ACLI commands

This feature introduces the following ACLI commands:

- ipv6 autoconfig
- no ipv6 autoconfig
- default ipv6 autoconfig
- ipv6 icmp addr-unreach
- no ipv6 icmp addr-unreach
- default ipv6 icmp addr-unreach
- ipv6 icmp port-unreach
- no ipv6 icmp port-unreach
- default ipv6 icmp port-unreach
- ipv6 nd hop-limit
- ipv6 nd dad-ns
- clear ipv6
- default ipv6 mgmt interface process-redirect
- ipv6 mgmt interface process-redirect
- no ipv6 mgmt interface process-redirect
- show ipv6 destinationcache
- show ipv6 default-routers
- show ipv6 mld-host-cache

- show ipv6 nd interface
- show ipv6 nd-prefix interface

For more information about ACLI commands, see *ACLI Commands Reference for Avaya Virtual Services Platform 7000 Series*, NN47202–600.

IPv6 loopback

IPv6 loopback provides support for loopback IPv6 interface on switch/stack. A maximum of 4 internal loopback Ipv6 interfaces can be configured to test IPv6 stack applications prior to connection to other devices.

For information about configuring the IPv6 loopback, see *Configuring Layer 2 on Avaya Virtual Services Platform 7000 Series*, NN47202–502.

ACLI commands

This feature introduces the following ACLI commands:

- ipv6 interface enable
- ipv6 interface address
- no ipv6 interface address
- no ipv6 interface

For more information about ACLI commands, see *ACLI Commands Reference for Avaya Virtual Services Platform 7000 Series*, NN47202–600.

SLPP Guard on trunk

The SLPP Guard on trunk feature provides loop protection on ports that belong to MLT, DMLT, or LAC trunks.

When SLPP Guard state or timeout of a port is configured, the SLPP Guard on trunk checks if the port belongs to an MLT or LAC trunk, in which case the settings are propagated on all ports that belong to that trunk.

For more information, see *Configuring Layer 2 on Avaya Virtual Services Platform 7000 Series*, NN47202–502.

SMLT and static MAC addresses

Static MAC addresses inserted on an SMLT port/trunk migrate to IST at SMLT DOWN event, and back at local SMLT UP event.

When the local SMLT port/trunk goes down, all static MAC addresses inserted on that port/trunk migrate to the IST trunk to ensure a correct flow of traffic. This occurs when the remote SMLT is up or down.

When the SMLT port/trunk is back up, the MAC addresses are migrated back.

Note:

SMLT task does not insert Static MAC addresses on a peer. The static MAC addresses should be inserted on both cores on the SMLT trunk/port.

SPB node scaling to 1000

Allowable scaling in the network extends from 500 nodes to 1000 nodes.

Transparent UNI over static SMLT

Release 10.4 supports Transparent UNI over static SMLT. In order for a Transparent UNI to work correctly in a SMLT configuration, the same ISID must be configured on both SMLT peers. When an ISID that has Transparent UNIs on only one of the two SMLT peers is configured, a transparent smlt-peer UNI on the other SMLT peer must also be created.

For more information, see *Configuring Avaya Fabric Connect on Avaya Virtual Services Platform 7000 Series*, NN47202–510.

Obsolete features

Fiber Channel over Ethernet (FCoE) solution is not supported in Release 10.4. The last supported release is Release 10.3.3.

Other changes

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

Unsupported MIBs

The following MIBs are not supported in Release 10.4:

- ntnQosPolicyDiagsEntry from ntnQosPolicyDiagsTable
- ntnQosFilterLimitingAdminEnabled
- ntnQosFilterLimitingOperEnabled
- ntnQosUserPolicyNextFree
- ntnQosFilterStatsInProfileOctets
- ntnQosCountActOctets

Filter resource consumption

Filter resource consumption is updated to include application mask and filter resource requirements for IGMP Snooping and to include a list of features that cannot be configured if no Filter Manager resources are available after an upgrade.

For more information, see Filter resource consumption on page 66.

EDM support for Storm Control

In Release 10.4, EDM support is added for Storm Control. For more information, see *Configuring Security on Avaya Virtual Services Platform 7000 Series*, NN47202–501.

Chapter 3: Important notices

This section provides important software and hardware related notices.

Warnings and important notices

The following sections provides warning notices and important notices for the VSP 7000 Series.

Agent upgrade notice

Caution:

DATA LOSS CAN OCCUR — Do not upgrade directly from Release 10.0 to Release 10.2 or later.

If the switch is running Release 10.0, you must upgrade to Release 10.1 before upgrading to 10.2 or later software. Upgrading from Release 10.0 to the current release can cause accidental erasure of the agent image on the switch. If the primary agent image is erased, during the next reboot the switch attempts to boot from the secondary agent image.

Fabric Interconnect cables notice

Important:

You must orient each cable so that the alignment slot on the FI cable connector is correctly aligned with the switch. The FI cable alignment slot must be facing upwards. For more information, see the following figures.

Warning:

Risk of equipment damage

Incorrect FI cable insertion can cause physical damage to the VSP 7000 Series switch. For more information, see the following figures.

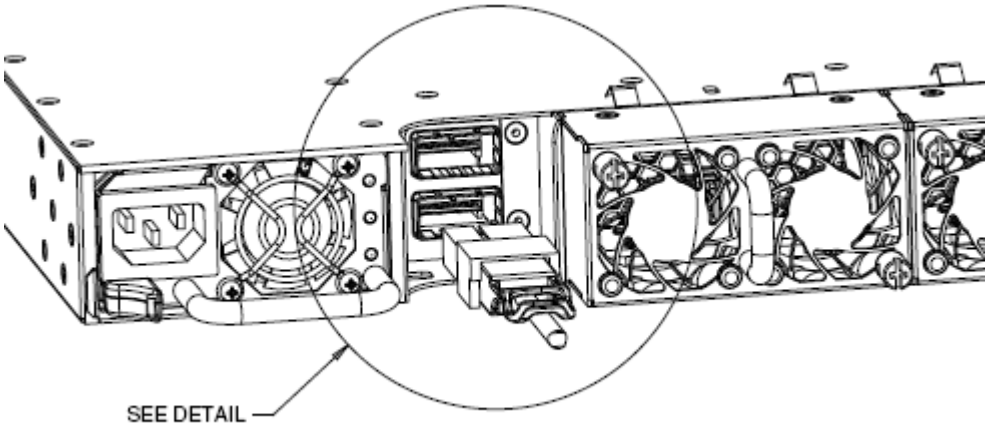
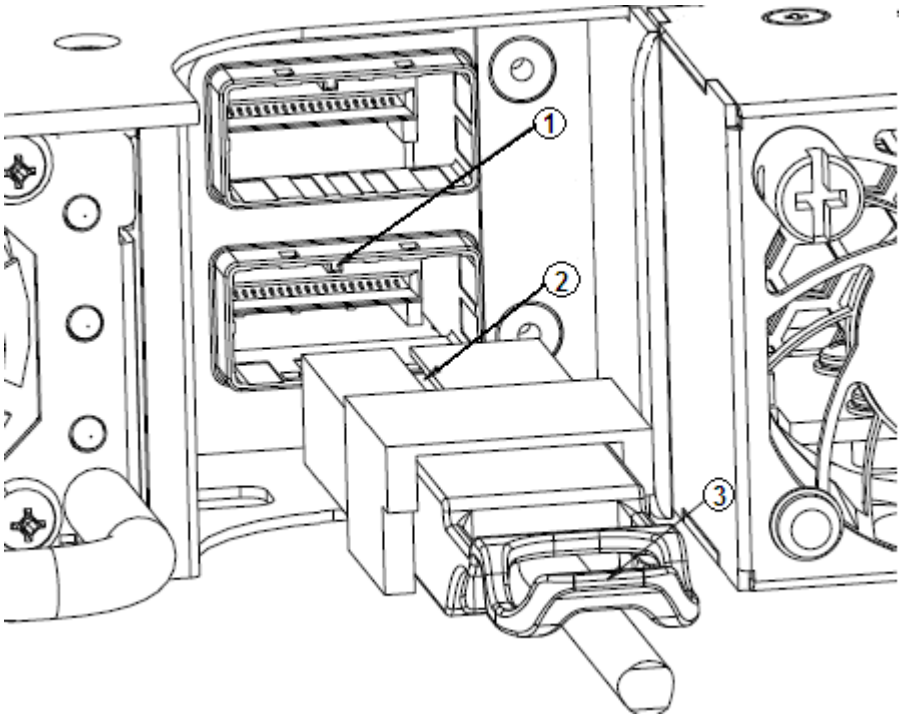


Figure 1: Installing Fabric Interconnect cables



Callout	Description
1	FI port alignment tab
2	FI cable alignment slot (Insert cable with slot facing UP and aligned with tab on the port)
3	FI cable connector pull tab (Ensure that the connector pull tab is facing UP)

Figure 2: Installing Fabric Interconnect cables detail

Important:

Remove the FI cables before changing between stacking and rear-port modes, or before fully defaulting a switch to avoid network loops.

Important:

A binary configuration saved on a Rear-port mode enabled unit cannot be restored on a unit that is not running in Rear-port mode. The operating mode of the VSP 7000 must match the binary configuration. You must manually configure the unit to the appropriate mode before you retrieve the binary configuration.

Important:

Rear port links might fail between units running different software builds. Rear-port mode operation is modified in Feature Pack Release 10.2.1 and later.

Note:

Avaya recommends upgrading all VSP 7000 Series units to the latest software release to ensure rear port mode compatibility between units.

Media Dependent Adaptor notice

Important:

Inserting the MDA might require a larger than anticipated amount of force to fully seat the MDA into the MDA slot. To ensure that the MDA is fully inserted, securely install the switch chassis in an equipment rack before installing the MDA.

Warning:

Risk of equipment damage

Do not apply vertical pressure when you insert and remove the transceiver. Improper installation can cause damage to the connector.

Warning:

Risk of equipment damage

If the MDA is not fully seated, do not use the thumb screws in an attempt to pull in the MDA. This can deform the front metal surround of the MDA.

Note:

The VSP–7008XT- MDA only supports full duplex mode of operation. Half duplex is not supported on 10GBASE-T ports.

Power Supplies recommendation

Avaya recommends the installation of two VSP 7000 power supplies to ensure minimum disruptions due to power outages.

File names for this release

The following table describes the Avaya Virtual Services Platform 7000 Series Release 10.4 software files. File sizes are approximate.

Module or file type	Description	File name	File size (bytes)
Standard runtime image for Release 10.4	Agent software image for the Avaya Virtual Services Platform 7000 Series	7000_1040003s.img—secure image	13,064,852
Diagnostics software for Release 10.4	Diagnostics software for the Avaya Virtual Services Platform 7000 Series	7000_10315_diags.bin — diagnostics	4,136,976
MIB definition files for Release 10.4	MIB definition files	Virtual_Services_Platform_7000_MIBs_10.4.zip	1,362,181
EDM Help files for Release 10.4	EDM help files	vsp7000v1040_HELP_EDM.zip	3,224,362

Software and hardware capabilities

The following table lists supported software and hardware scaling capabilities for the Avaya Virtual Services Platform 7000 Series Software Release 10.4.

The information in this table supersedes information contained in other technical documentation for VSP 7000 Series.

Feature	Maximum number supported
General	
Fabric Interconnect Stack-mode DToR bandwidth (8 units)	5,120 Gbps (full duplex)
Fabric Interconnect Stack-mode DToR (number of units).	8
Fabric Interconnect Fabric-mode DToR bandwidth (32 units)	20,480 Gbps (full duplex)
MDA supported on each VSP 7000	1
Layer 2	
Avaya Spanning Tree Groups	8
DHCP Snooping table entries	1,024
MAC addresses	131,071 (32,767 with SMLT)

Table continues…

Feature	Maximum number supported
Multi-Link Trunking (MLT), Distributed Multi-Link Trunking (DMLT), and Link Aggregation (LAG) groups	64
MLT Links or ports per MLT, DMLT, or LAG	8
MLT Maximum MAC Learning rate on an MLT trunk	2000 new MAC addresses per second
Spanning Tree Group instances (802.1s)	8
Static MAC addresses	1,024
VLAN Concurrent VLANs	1024
VLAN Protocol-based VLANs	16 PIDs
VLAN Supported VLAN IDs	1–4094 • 4001 reserved by STP • 4002–4008 reserved by multiple STP groups
Layer 3	
Maximum number of configurable loopback interfaces	16
IP interfaces (VLANs or Brouter ports)	256
ARP Entries total (local, static, and dynamic)	4,096
ARP Entries — local (IP interfaces for each switch or stack)	256
ARP Entries — static	256
IPv4 Routes total (local, static, and dynamic)	4,096
IPv4 Local Routes	256
IPv4 Static Routes	512
IPv6 interfaces	256
IPv6 neighbors total (local, static, and dynamic)	4,096
IPv6 static neighbors	256
IPv6 static routes	512
IPv6 in IPv4 tunnels (manually configured)	4
Dynamic Routing interfaces (RIP and OSPF)	64
OSPF Areas	4 (3 areas plus area 0)
OSPF Adjacencies	64
OSPF Link State Advertisements (LSAs)	10,000
OSPF Virtual Links	16
OSPF Host Routes	32
ECMP (Max concurrent equal cost paths)	4
ECMP (Max next hop entries)	4,096

Table continues…

Feature	Maximum number supported
VRRP instances	255 IDs (64 active)
Management Routes	4
UDP Forwarding Entries	128
DHCP Relay Entries	256
DHCP Relay Forward Paths	512
Multicast	
IGMP v1/v2 multicast groups	up to 1,024 (for 1,024 distinct streams) **Note:** These limits do not indicate that 1,024 entries are actually available because the installation of IP Multicast entries in hardware is also determined by the available free entries. One IP Multicast table is shared between multicast applications.
Quality of Service	
Egress queues	Configurable 1–8
Egress queues (Lossless Mode)	2
QoS rules	Precedence levels (slices); 10 Max QoS policies per port: 8 Max Filters per precedence: 128 (Precedence 1–4) Max Filters per precedence: 256 (Precedence 5–10) Max Meters per precedence: 128 Max Counters per precedence: 64 (Precedence 1–4) Max Counters per precedence: 128 (Precedence 5–10) Range Check Entries: 32 Traffic-profile classifiers: 1024 Traffic-profile sets: 512
QoS Traffic Profile Criteria — Layer 2 **Note:** Traffic Profiles provide the combined benefits of ACLs, Filters, and Classifiers.	• Source MAC address/mask • Destination MAC address/mask • VLAN ID range • VLAN tag • EtherType • Packet type • 802.1p priority values

Table continues…

Feature	Maximum number supported
QoS Traffic Profile Criteria — IPv4	• IPv4 source address/mask • IPv4 destination address/mask • IPv4 address type • IPv4 protocol type • IPv4 DSCP value • IPv4 source TCP port range • IPv4 source UDP port range • IPv4 destination TCP port range • IPv4 destination UDP port range • IPv4 flags • TCPv4 control flags • IPv4 options
QoS Traffic Profile Criteria — IPv6	• IPv6 source address/mask • IPv6 destination address/mask • IPv6 address type • IPv6 flow identifier • IPv6 next-header • IPv6 DSCP value • IPv6 source TCP port range • IPv6 source UDP port range • IPv6 destination TCP port range • IPv6 destination UDP port range
QoS elements — System	• unknown IP multicast • known IP multicast • unknown non-IP multicast • known non-IP multicast • non-IP packet • unknown unicast packet
Switch Cluster (SMLT)	
Switch Cluster: operational mode	Standalone or Stack
Switch Cluster: configuration	Triangle or Square
Switch Cluster: MLT uplinks	32
Switch Cluster: SLT uplinks	128

Table continues…

Feature	Maximum number supported
Switch Cluster: SMLT/LACP uplinks	20
Switch Cluster: SLT/LACP links	100
Switch Cluster: SLPP VLANs	20
Switch Cluster: IST using LACP	Not supported in this release
Switch Cluster: IST/LACP	Not supported in this release
Switch Cluster: Static IP Routes supported across IST	Supported
Switch Cluster: Static IP Routes over SLT/MLT links	Supported
Switch Cluster: Dynamic IP Routing over IST links	Supported
Switch Cluster: Dynamic Routing protocol over Switch Cluster (OSPF and RIP over SMLT)	Standalone or Stack: • 64 OSPF/RIP interfaces • 4 OSPF area • 4096 routes • 4096 ARPs • 64 VRRP instances, no FAI • ECMP supported • Rear-port mode supported
Switch Cluster: IGMP over SMLT	Supported
Switch Cluster: Fabric Connect over SMLT	Supported
Switch Cluster: SMLT/IST over rear ports in Raw-mode	Supported
Fabric Connect (SPB)	
Fabric Connect: operational mode	Standalone or stack
Fabric Connect: Customer VLANs (C-VLANs) per node	500 for stacks with or without SMLT, and standalone with SMLT 800 for standalone without SMLT
Fabric Connect: ISIDs per node	1000
Fabric Connect: Switched UNIs	4096
Fabric Connect: nodes per region	Max nodes: 1000 Nodes with ISIDs in common: 500 without SMLT 500 less 1 for each SMLT node pair, to a limit of 340 for SPBM over SMLT in a 340 node, 100% SMLT network
Fabric Connect: (IS-IS) adjacencies per node	24
Miscellaneous	

Table continues…

Feature	Maximum number supported
IGMP Enabled VLANs	256
HTTP Server IPv4	3 sessions
HTTP Server IPv6	3 sessions
IPFix number of sampled flows	100,000
LLDP Neighbors	800
LLDP Neighbors per port	16
Port Mirroring instances	4
RMON alarms	800
RMON Ethernet history	249
RMON Ethernet statistics	110
RMON events	800
Telnet Client IPv6	4 sessions
Telnet Server IPv6	4 sessions

Supported browsers

Virtual Services Platform 7000 supports the following browsers to access the Enterprise Device Manager (EDM):

- Microsoft Internet Explorer 7.x
- Microsoft Internet Explorer 8.x
- Mozilla Firefox 3.x and up

Note:

Due to an issue in Firefox versions greater than 3.6.x, you might not be able to import SSL certificates using IPv6. As a workaround, you can use the hostname (with host IPv6 address resolved by DNS or editing the local hosts file), or use Microsoft Internet Explorer 8.x.

Upgrading switch software using ACLI

Use this procedure to specify the download target image and change the software version running on the switch.

About this task

You can update either of the following:

- the active software image
- the non-active software image

Caution:

DATA LOSS CAN OCCUR — Do not upgrade directly from Release 10.0 to Release 10.2 or later.

If the switch is running Release 10.0, you must upgrade to Release 10.1 before upgrading to 10.2 or later software. Upgrading from Release 10.0 to the current release can cause accidental erasure of the agent image on the switch. If the primary agent image is erased, during the next reboot the switch attempts to boot from the secondary agent image.

The software image download process occurs automatically within a stack if different software is present. This process deletes the contents of the flash memory and replaces it with the specified software image.

Tip:

To track the progress of the download process, you can observe the switch front panel LEDs.

Depending on network conditions, the download process may take up to 10 minutes.

Important:

Do not interrupt the download process.

You can update the runtime image (agent code) on the switch while the switch is operational. If you specify the no-reset option, the new software is updated on FLASH, but is not running on the switch. If you do not specify the no-reset option, once the download of switch software is complete, the switch or Fabric Interconnect Stack resets and restarts with the new image.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   download [address <A.B.C.D|<WORD> | tftp address <A.B.C.D|<WORD> |
   sftp address <A.B.C.D| <WORD> | usb] [primary | secondary] [image
   <image_name> | image—if—newer <image_name> | diag <image_name>] [no-
   reset]
   ```

   Note:

   If you use the download command without the optional parameters, the switch prompts you to provide the necessary information. The switch maintains a memory and can reuse the last information entered for the download command. To reuse information, press **Enter** when the switch prompts you to provide details rather than typing the information.

   Note:

   When you upgrade a switch or stack running VLACP do not use the "no Reset" option on the download command. VLACP may bounce due to missed PDUs during the download process.

Example

Upgrade the diagnostics.

```
7024XLS>enable
7024XLS#download address 192.0.2.1 diag 7000_10201_diags.bin
```

Upgrade the switch image using an SFTP server.

```
7024XLS>enable
7024XLS#download sftp address 192.0.2.1 primary image 7000_1021049s.img
```

Variable definitions

The following table describes parameters to help you use the **download** command to upgrade agent software.

Variable	Value
address <*A.B.C.D*|<*WORD*> | tftp address <*A.B.C.D*| <*WORD*> | sftp address <*A.B.C.D*| <*WORD*> | usb	Specifies the IPv4 or IPv6 address of the server on which the agent image is hosted. • A.B.C.D — Specifies the IP address in IPv4 format. • WORD — Specifies the IP address in IPv6 format. The address parameter is optional and, if omitted, the switch defaults to the TFTP server specified by the **tftpserver** command unless software download is to take place using a USB mass storage device. The sftp address parameter appears only if the switch runs a secure image.
primary | secondary	Specifies the image to download: primary or secondary.
image<*image_name*>	Specifies the name of the software image file to be downloaded from the TFTP server.
image—if—newer <*image_name*>	Specifies the name of the software image to be downloaded from the TFTP server if newer than the currently running image.
diag <*image_name*>	Specifies the name of the diagnostic image to be downloaded from the TFTP server.
no-reset	Stops the switch from resetting after completion of the software download.
Note: The image, image-if-newer, and diag parameters are mutually exclusive and you can execute only one at a time.	

Upgrading switch software using EDM

Use the following procedure to change the software version running on the switch using Enterprise Device Manager (EDM).

Caution:

DATA LOSS CAN OCCUR — Do not upgrade directly from Release 10.0 to Release 10.2 or later.

If the switch is running Release 10.0, you must upgrade to Release 10.1 before upgrading to 10.2 or later software. Upgrading from Release 10.0 to the current release can cause accidental erasure of the agent image on the switch. If the primary agent image is erased, during the next reboot the switch attempts to boot from the secondary agent image.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **File System**.
3. In the work area, click the **Config/Image/Diag file** tab.
4. Configure the parameters required to perform the image download.
5. On the toolbar, click **Apply**.

Result

The software download occurs automatically once you click Apply. This process erases the contents of the flash memory and replaces it with the new software image.

Important:

Do not interrupt the download. Depending on network conditions, this process can take up to 10 minutes.

When the download is complete, the switch automatically resets and the new software image initiates a self test.

Important:

During the download process, the management functionality of the switch is locked. Normal switching operations continue to function until the switch resets.

Variable definitions

The following table describes updating the binary configuration, image, and diagnostic files.

Variable	Value
TftpServerInetAddressType	Specifies the IP address type of the TFTP or SFTP server. Values include IPv4 or IPv6.

Table continues…

Variable	Value
TftpServerInetAddress	Specifies the IP address of the TFTP or SFTP server.
BinaryConfigFilename	Specifies the binary configuration file currently associated with the switch. This field only applies to binary configuration files.
BinaryConfigUnitNumber	Specifies the unit number portion of the configuration file to be used for the standalone unit configuration. Values range from 0 to 8. If 0, the unit number is ignored. This field only applies to binary configuration files.
ImageFileName	Specifies the name of the image file currently associated with the switch. You can change this field to the filename of the software image to be downloaded.
FwFileName(Diagnostics)	Specifies the name of the diagnostic file currently associated with the switch. You can change this field to the filename of the software image to be downloaded.
Usb TargetUnit	Specifies the unit number for USB, or the transfer type to use during the upload or download operation. Values include: • 1 to 8 — USB on unit 1 to 8 • 9 — USB on a standalone unit • 0 — TFTP server • 10 — SFTP server
Image	Specifies if the image to download is the primary or secondary image.
Action	Specifies the action to perform during the file transfer. Values include: • dnldConfig — Downloads the configuration file from a TFTP or SFTP server • upldConfig — Uploads the configuration file to a TFTP or SFTP server • dnldConfigFromUsb — Downloads the configuration file from a USB storage device. • upldConfigToUsb — Uploads the configuration file to a USB storage device. • dnldImg — Downloads the agent image file from a TFTP or SFTP server.

Table continues…

Variable	Value
	• dnldImgIfNewer — Only downloads if newer than current image. • dnldImgNoReset — Downloads the agent image and does not reset the switch. • dnldImgFromUsb — Downloads the agent image from a USB storage device. • dnldFw — Downloads the diagnostic image from a TFTP or SFTP server. • dnldFwNoReset — Downloads the diagnostic image and does not reset the switch. • dnldFwFromUsb — Downloads the diagnostic image from a USB storage device. • dnldImgFromSftp — Downloads the agent image from a SFTP server. • dnldFwFromSftp — Downloads the diagnostic image from a SFTP server. • dnldConfigFromSftp — Downloads the configuration file from a SFTP server. • upldonfigToSftp — Uploads the configuration file to a SFTP server. • dnldImgFromSftpNoReset — Downloads the agent image from a SFTP server and does not reset the switch. • dnldFwFromSftpNoReset — Downloads the diagnostic image from a SFTP server and does not reset the switch.
Status	Indicates the status of the last action since the last switch reboot. Values include: • other — No action has taken place. • inProgress — The selected action is currently in process. • success — The selected action completed successfully. • fail — The selected action failed.

Supported standards, MIBs, and RFCs

This section lists the standards, MIBs, and RFCs supported by the Avaya Virtual Services Platform 7000 Series.

Standards

The following IEEE Standards contain information that applies to the Avaya Virtual Services Platform 7000 Series.

- IEEE 802.1 — Port VLAN, Port and Protocol VLANs, VLAN Name, Protocol Entity
- IEEE 802.1AB — Layer Link Discovery Protocol
- IEEE 802.1aq — Shortest Path Bridging
- IEEE 802.1ax — Link Aggregation Control Protocol
- IEEE 802.1D — Standard for Spanning Tree Protocol
- IEEE 802.1p — Prioritizing
- IEEE 802.1Q — VLAN Tagging
- IEEE 802.1s — Multiple Spanning Tree Protocol
- IEEE 802.1v — VLAN Classification by Protocol and Port
- IEEE 802.1w — Rapid Spanning Tree Protocol
- IEEE 802.3 — Ethernet
- IEEE 802.3ab — Gigabit Ethernet over Copper
- IEEE 802.3ad — Link Aggregation
- IEEE 802.3ae – 10 Gbps Ethernet
- IEEE 802.3aq — Ethernet over multimode fiber
- IEEE 802.3x — Flow Control
- IEEE 802.3z — Gigabit Ethernet over Fiber-Optic

RFCs and MIBs

For more information about networking concepts, protocols, and topologies, consult the following RFCs and associated MIBs:

- RFC 768 (UDP)
- RFC 791 (IP)
- RFC 792 (ICMP)
- RFC 793 (TCP)

- RFC 826 (ARP)
- RFC 854 (Telnet)
- RFC 894 (IP over Ethernet)
- RFC 950 (Subnetting)
- RFC 951 (BootP)
- RFC 1058 (RIP v1)
- RFC 1112 (IGMPv1)
- RFC 1157 (SNMP)
- RFC 1213 (MIB-II)
- RFC 1215 (SNMP Traps Definition)
- RFC 1271 (RMON)
- RFC 1305 (NTP v3)
- RFC 1350 (TFTP)
- RFC 1493 (Bridge MIB)
- RFC 1583 (OSPF v2)
- RFC 1757 (RMON)
- RFC 1769 (SNTP)
- RFC 1850 (OSPF v2 MIB)
- RFC 1886 (DNS Extensions for IPv6)
- RFC 1905 (SNMP)
- RFC 1906 (SNMP Transport Mappings)
- RFC 1907 (SNMP MIB)
- RFC 1945 (HTTP v1.0)
- RFC 1981 (Patch MTU Discovery for IPv6)
- RFC 2011 (SNMPv2 IP MIB)
- RFC 2012 (SNMPv2 TCP MIB)
- RFC 2013 (SNMPv2 UDP MIB)
- RFC 2131 (BootP/DHCP Relay Agent)
- RFC 2236 (IGMPv2)
- RFC 2328 (OSPF v2)
- RFC 2453 (RIP v2)
- RFC 2460 (IPv6)
- RFC 2464 (Transmission of IPv6 packets over Ethernet networks)

- RFC 2474 (DiffServ)
- RFC 2475 (DiffServ)
- RFC 2665 (Ethernet MIB)
- RFC 2674 (Q-BRIDGE-MIB)
- RFC 2737 (Entity MIBv2)
- RFC 2819 (RMON MIB)
- RFC 2863 (Interfaces Group MIB)
- RFC 2865 (RADIUS)
- RFC 2866 (RADIUS Accounting)
- RFC 2933 (IGMP MIB)
- RFC 3046 (DHCP Relay Agent information option)
- RFC 3162 (RADIUS and IPv6)
- RFC 3246 (Expedited Forwarding Behavior)
- RFC 3315 (IPv6 DHCP Relay)
- RFC 3410 (SNMPv3)
- RFC 3411 (SNMP Frameworks)
- RFC 3412 (SNMP Message Processing)
- RFC 3413 (SNMPv3 Applications)
- RFC 3414 (SNMPv3 USM)
- RFC 3415 (SNMPv3 VACM)
- RFC 3416 (SNMP)
- RFC 3417 (SNMP Transport Mappings)
- RFC 3418 (SNMP MIB)
- RFC 3584 (Coexistence of SNMPv1/v2/v3)
- RFC 3768 (VRRP)
- RFC 3917 (IPFix)
- RFC 3954 (Netflow Services Export v9)
- RFC 3993 (DHCP Subscriber-ID suboption)
- RFC 4007 (Scoped Address Architecture)
- RFC 4022 (TCP MIB)
- RFC 4113 (UDP MIB)
- RFC 4213 (IPv6 in IPv4 tunnels)
- RFC 4250 (SSH Protocol assigned numbers)

- RFC 4251 (SSH Protocol architecture)
- RFC 4252 (SSH Authentication Protocol)
- RFC 4253 (SSH Transport Layer Protocol)
- RFC 4254 (SSH Connection Protocol)
- RFC 4291 (IPv6 addressing architecture)
- RFC 4293 (IPv6)
- RFC 4432 (SSH RSA)
- RFC 4443 (ICMPv6)
- RFC 4541 (Considerations for IGMP and MLD snooping switches)
- RFC 4604 (IGMPv3)
- RFC 4861 (Neighbor Discovery for IP version 6)
- RFC 4862 (IPv6 Stateless Address Autoconfiguration)
- RFC 5905 (Network Time Protocol Version 4)
- RFC 6724 (Default Address Selection for Internet Protocol Version 6)

Chapter 4: Resolved issues

Use the information in this section to learn more about issues that have been resolved.

Resolved issues for Release 10.4

The following table lists the issues resolved in Release 10.4.

Reference number	Description
wi01190811	Intra-stack communication failure error returned constantly on a 3-high stack when trying to save the binary config to tftp. **This issue was resolved in this release.**
wi01219321	Default static route is removed in HW after Firewall Failover (duplicate IP). **This issue was resolved in this release.**
wi01212681	VSP 7000 10.3.2: tGbic task is taking 10% which is making overall CP util to be at 30-40%. **This issue was resolved in this release.**
wi01162798	Resetting to partial-defaults erases the static IP mgmt routes. **This issue was resolved in this release.**
wi01205023	OSPF communication fails from any modular (8600 or VSP9k) to VSP 7000 if LSA Type 1 contains more than 242 link entries. **This issue was resolved in this release.**
wi01206463	Switch asks to change the password even when the 'password security' feature is disabled. **This issue was resolved in this release.**
wi01209880	PING loss due to MAC FLAPPING. **This issue was resolved in this release.**
wi01207300	Forwarding issues over non-ist vlan. **This issue was resolved in this release.**
wi01219077	Routing issue when link flaps. **This issue was resolved in this release.**

Table continues…

Reference number	Description
wi01224233	MIB walk shows incorrect port while MAC learned on different port. **This issue was resolved in this release.**
wi01224612	VSP7000 - 10.3.1 & 10.3.3 - SPBM - l2pings fail on primary & secondary BVLAN, l2traceroutes do not include the last hop of destination BEB. **This issue was resolved in this release.**
wi01225969	VSP7K stuck in loop displaying the same SPBM MAC after I-SID was removed. **This issue was resolved in this release.**
wi01173968	Both IST partners experience stack fail when setting one of then to partial default and then loading the ASCII configuration file. **This issue was resolved in this release.**
wi01198684	IST/SMLT not recovering after boot default, load ASCII config and boot BU. **This issue was resolved in this release.**
wi01192603	OOB mgmt route is not working for NBU (2nd unit) from stack running in stack forced-mode. **This issue was resolved in this release.**
wi01188883	AUTO: Unable to login through SSH using an username with more than 17 characters (Radius Authentication). **This issue was resolved in this release.**
wi01187310	IP mgmt route configured for in-band interface is not functional in TBU mode. **This issue was resolved in this release.**
wi01178220	EDM: missing speed 40000 and 40000-full auto-negotiation advertisement from the interface tab for QQ-MDA ports. **This issue was resolved in this release.**
wi01174049	“speed 40000” command settings are removed from the running-config after disconnect/re-connect the 40Gig DAC **This issue was resolved in this release.**
wi01173968	Both IST partners experience stack fail when setting one of then to partial default and then loading the ASCII configuration file. **This issue was resolved in this release.**
wi01170262	show who does not display all sessions if multiple sessions are used from same source via SSH. **This issue was resolved in this release.**
wi01170238	CLI: Module "aaa" not available when using script upload. **This issue was resolved in this release.**
wi01164344	SPBM: Configuration is corupted after disabling lacp with static key binding on a NNI.

Table continues…

Reference number	Description
	This issue was resolved in this release.
wi01164343	SPBM/SMLT: ISIS can be enabled on LACP with SMLT ports. **This issue was resolved in this release.**
wi01164341	ISIS: Adjacencies keep bouncing at one edge after changing lacp key binding at the other edge of the LAG trunk. **This issue was resolved in this release.**
wi01153467	Logging: space alignment issue for Enabling trunk ports. **This issue was resolved in this release.**
wi01152207	TDR doesn't work for VSP 7024XT ports. **This issue was resolved in this release.** **Note:** Feature is no longer supported on the VSP7024.
wi01144333	100% CPU utilization and adjacencies bounce after stack with SPBM over SMLT with 250 CVLANs after reset. **This issue was resolved in this release.**
wi01142083	Rear ports may not be up if inserting fiber cable simultaneously in both peers after units are powered up (intermittent). **This issue was resolved in this release.**
wi01140826	SMLT: Smlt Link Down traps are doubled when IST peer is powered off. **This issue was resolved in this release.**
wi01136953	DAI Traps: "bsaiArpPacketDroppedOnUntrustedPort" trap is sent with wrong "bsArpInspectionIfTrusted" object value. **This issue was resolved in this release.**
wi01129022	USB:SanDisk Ultra Backup 64GB doesn't work on build 10.3.0.125. **This issue was resolved in this release.**
wi01122796	When password is changed via EDM to local/TACACS for serial/telnet no syslog message is generated. **This issue was resolved in this release.**
wi01122504	EDM offbox: timed out received when accessing LLDP Avaya Local File Server if file servers are configured (ok in EDM). **This issue was resolved in this release.**
wi01119577	New:RSPAN: Traffic is not mirrored for some ports in Xtx and manytoonetx modes through RSPAN. **This issue was resolved in this release.**
wi01104171	NEW: RSPAN - Incorrect tag when add multiple RSPAN vlans with different monitor ports.

Table continues…

Reference number	Description
	This issue was resolved in this release.
wi01089102	Rear-ports: Incorrect auto-negotiation-advertisements setting for rear ports are found in running config (ASCII fails). **This issue was resolved in this release.**
wi01085751	SMLT:Traffic recovers in 90s on BU down and 40 seconds when unit1 rejoins the stack (L2 flood in both cases for 30-40 seconds). **This issue was resolved in this release.**
wi01042491	Adding one port to 1000 vlans takes more than 5 minutes. **This issue was resolved in this release.**
wi00985066	VSP7000 R10.1 Trials: Same OID returned two different values. **This issue was resolved in this release.**
wi00930939	Ping from CLI to DUT ip does not work after changing ip netmask (starting with build 056). **This issue was resolved in this release.**
wi01142083	**Rear-ports**: Rear ports may not be up if inserting fiber Stack cable simultaneously in both peers after units are powered up (intermittent). **This issue was resolved in this release.**
wi01200517	QoS agent buffer=LossLess: Can't set on rear ports 33-40 flow control=symmetric if FO stack cables are used. **This issue was resolved in this release.**
wi01192603	OOB mgmt route is not working for Non Base unit (2nd unit) from stack running in stack forced-mode. **This issue was resolved in this release.**
wi01186969	SMLT aggregation DUT BU resets with “PP” DAE and IST down if send CPU intensive traffic in MGMT VLAN over SMLTs **This issue was resolved in this release.**
wi01164343	**SPBM/SMLT**: ISIS can be enabled on LACP with SMLT ports. This should be blocked as it is unsupported. **This issue was resolved in this release.**
wi01137103	The fix consists in migrating static mac addresses from SMLT ports on IST ports when SMLT ports are down. Also when SMLT ports are up again, the static mac addresses are migrated from IST ports on SMLT ports. For Microsoft NLB to work, user must add the virtual mac address static only on SMLT (MLT) on both peers. **This issue was resolved in this release.**

Resolved issues for Release 10.3.3

The following table lists the issues resolved in Feature Pack Release 10.3.3.

Reference number	Description
wi01175455	Rear-port mode: speed & auto-neg-adv commands generated by ACG for ports 33-40 are failing. **This issue was resolved in this release.**
wi01170218	Rate-limit on 40 Gig port doesn't work for percent 6 or higher. **This issue was resolved in this release.**
wi01188057	New Sflow: In EDM there is no option to default on ports sflow IngressSamplingRate, EgressSamplingRate and Counter Pooling. **This issue was resolved in this release.**
wi01191814	After power-cycle SMLT aggregation stack, tSnmpt task keeps the CPU on non-BUs at 100% utilization. (Very intermittent). **This issue was resolved in this release.**
wi01179141	Memory Leak in the Base Unit makes the unit non-responsive and resulting in failover when WoL (wake on Lan) is performed on many clients. **This issue was resolved in this release.**
wi01187416	Using sflow sampling: Not entire DHCP packet is displayed (max 256 bytes) or malformed. Egress unicast DHCP relay packets are not captured. **This issue was resolved in this release.**
wi01184748	SBPM NNI failover times get much worse as the LSDB increases. **This issue was resolved in this release.**
wi01191266	SBR based on TCP/UDP ports is not working. **This issue was resolved in this release.**
wi01177034	After upgrading the VSP 7000 core to 10.3.0.11, the DHCP-replay counters are not incrementing in one of the VSP 7000 core. **This issue was resolved in this release.**
wi01017518	Failover in IS-IS mesh topology is over 5 seconds. **This issue was resolved in this release.**
wi01185709	VSP 7000 T-UNI port not passing VRRP/OSPF control traffic. **This issue was resolved in this release.**
wi01102846	**SMLT/VLACP**: SMLT aggregation units become unresponsive and cannot be used after enabling VLACP on all SMLTs. **This issue was resolved in this release.**
wi01103003	**SMLT: SMLT / IST over Rear Ports**: Background traffic does not recover for approximately 80 seconds when disabling VLACP globally in an SMLT setup.

Table continues…

Reference number	Description
	This issue was resolved in this release.
wi01142085 wi01140095	**Rear-ports**: Speed mismatch (1000 Mbps - 40 Gbps) may be seen when swapping rear-port fiber cable with copper cable (intermittent). **This issue was resolved in this release.**
wi00930939	**Netmask**: Modifying the netmask without an IP address might result in connectivity loss. **This issue was resolved in this release.**
wi01175700	Traffic does not recover if disable/re-enable VLACP on SLT/SMLT interfaces. **This issue was resolved in this release.**
wi01183258	Auto: CLI command to create QoS queue-shaper does not work on stack (start with SW 10.3.2.035). **This issue was resolved in this release.**
wi01082016	**Rear-port mode:** Rear port links might fail between units running different Release 10.2 software builds. Rear-port mode operation is modified in Release 10.2.1 and later. **This issue was resolved in this release.**
wi00972061	**EDM, Fan Status LEDs:** When using Enterprise Device Manager (EDM), the Device physical view does not display the FAN status LED colors: only grey is displayed for the fan status. **This issue was resolved in this release.**
wi01029850	**L2Ping, CFM:** Due to system timing on the VSP 7000, the roundtrip times (minimum, maximum, and average) displayed from L2ping show higher values than other platforms, such as the VSP 9000 and ERS 8800. **This issue was resolved in this release.**
wi01042491	**VLAN:** Adding one port to 1000 VLAN might take an extended period of time. **This issue was resolved in this release.**
wi01119793	**ASCII script**: auto download does not work from SFTP using ASCII script. **This issue was resolved in this release.**
wi01153463	**MDA 40Gb:** MDA ports are flapping when resetting a peer. **This issue was resolved in this release.**
wi01175650	**EDM:** There is no option for mbps40000 under AdminSpeed for 40G interfaces. **This issue was resolved in this release.**
wi01176877	**BETA EDM:** The color for fiber ports with no SFP/SFP+/QSFP connected does not become red after shutdown or MDA disable (is always grey). **This issue was resolved in this release.**

Table continues…

Reference number	Description
wi01178220	**EDM:** missing speed 40000 and 40000-full auto-negotiation advertisement from the interface tab for QQ-MDA ports. **This issue was resolved in this release.**

Resolved issues for Release 10.3.2

The following table lists the issues resolved in Feature Pack Release 10.3.2.

Reference number	Description
wi01177872	Change radius password feature isn't working from EDM.
wi01156851	**SPBM/SMLT**: SLPP may shut down LACP-based SLT ports on the C-VLAN after the IST peer that connects to other switching devices is reset.
wi01157808	**SPBM/SMLT**: LACP port-mode is toggled from Advanced Mode to default after an SLT is deleted or modified.
wi01157948	**SPBM**: For ARP entries in the **`show arp-table`** command output, the Unit/Port for the management I-SID is updated with VPID. When using management I-SID in SPBM, depending on the ports used, the output of the **`show arp-table`** command might not be accurate regarding Unit/Port values. This is a display issue only.
wi01160393	**MDA**: A VSP 7000 MDA 10GBASE-T port connected to Intel I35010G NIC may not come up at 10 Gbps.
wi01162796	**VSP7000**: Stack-of-2 Force stack-mode / IP mgmt routes become inactive after unit failure.
wi01164416	Autotopology returning wrong info for 8800.
wi01156843	SPBM/SMLT: Loss of management over C-VLAN from SMLT when the original base unit is down and the stack is running on a temporary base unit until the original base unit re-joins the stack. Workaround: None. This issue is intermittent.
wi01162789	VSP7000/MDA Hot Swap : Disabled MDA ports are automatically reenabled after hot-swap - Working as designed.
wi01167547	SPBM/QQ-MDA: Unable to ping over I-SID after installing QQ-MDAwhen running with SMLT over SPBM.
wi01172673	BU CPU stays at 100% utilization if you have CLIP configured to send SNMP traps and disable IP routing.
wi01148482	Lossless: 40G ports do not support pause-frames negotiation.
wi01146740	QoS: Meter capability up to 40 Gbps needed on some ports.
wi01146739	QoS: Shaper capability up to 40 Gbps needed on some ports.
wi01155692	40G MDA: Port links up at 10 Mbps. (intermittent) – Display Issue.
wi01168326	After upgrade from 10.3.1 to 10.3.2 the RW/RO passwords are 16 defaulted.

Resolved issues for Release 10.3.1

The following table lists the issues resolved in Feature Pack Release 10.3.1.

Reference number	Description
wi00979441	**Automation**: Intermittently configuration objects might change unexpectedly during a large number of random resets or power cycles. Changes are minor and not expected in customer configurations.
wi00974728	**VLACP, Traps**: Inconsistent logging of VLACP traps can occur if enabled.

Resolved issues for Release 10.3 and earlier

The following table lists the issues resolved in Release 10.3 and earlier.

Reference number	Description
wi01023541	**Lossless PFC mode**: In Lossless-PFC mode, regardless of flow control settings the port sends PFC frames on oversubscription. **This issue was resolved in this release.**
wi01049340	**QoS resources**: If a Release 10.1 unit with all QoS precedences used is upgraded to Release 10.2, the QoS policies will disable. This failure occurs because SPBM requires QoS precedence 9 even if SPBM is not configured. **This issue was resolved in this release.**
wi01059397	**FI ports**: If you change a switch configuration from FI stacking to FI rear-port mode, or vise versa, without removing the FI cables, there is a high probability of causing a loop across the FI ports. **This issue was resolved in this release.**
wi01043735	**SPBM, Port mirroring**: If you mirror a port with IS-IS enabled, the mac-in-mac 802.1ah header is stripped from all SPBM encapsulated packets. **This issue was resolved in this release.**
wi01039526	**SPBM, ERS 8800 Interoperability**: When connecting a VSP 7000 to an ERS 8800 running SPBM, IS-IS adjacencies are not formed with the ERS 8000, unless the ERS 8800 is running Release 7.1.3 or later. **This issue was resolved in this release.**

Table continues…

Reference number	Description
wi01040581	**Rear-port mode, full default**: If you fully default a switch operating in rear-port mode, the rear-port mode is disabled. Upon reboot, the fully defaulted unit attempts to join a FI stack, causing other connected units operating in rear-port mode to crash. **This issue was resolved in this release.**
wi01027055	**Rear-port mode, SPBM**: By default, all Fabric Interconnect ports operating in rear-port mode use the same LACP key. If you modify a rear-port metric, such as the SPBM-L1–Metric, the modification applies to all ports which are members of the same LAG. **This issue was resolved in this release.**
wi01031500	**Rear-port mode, ISIS:** The command `show isis interface` displays all rear-ports, irrespective of state, because all rear-ports are members of the same default LAG. **Duplicate. This issue was resolved with wi01031322.**
wi01114953	**Important:** **Rear-port mode**: The binary configuration saved on a Rear-port mode enabled unit cannot be restored on a unit that is not running in Rear-port mode. The operating mode of the VSP 7000 must match the binary configuration. **This issue was resolved in this release.**
wi01031322	**Rear-port mode, ISIS:** By default, all Fabric Interconnect ports operating in Rear-port mode use the same LACP key. If you enable ISIS on a rear-port, ISIS is enabled on all rear-ports. **This issue was resolved in this release.**
wi00998949, wi01042576	**OS, Agent upgrades**: **DO NOT UPGRADE DIRECTLY FROM RELEASE 10.0 TO CURRENT RELEASE**. **Warning:** Do not upgrade from Release 10.0 directly to Release 10.2 or later, the new agent image buffer is exceeded and primary agent image is erased. **This issue was resolved in this release.**
wi00888731	**Boot loader stops**: Intermittent. The diagnostic/boot/agent loader might stop on boot after a switch or stack reset or upgrade.
wi00971049	**Automation**: Intermittent, Error tCliAudit errors writing to flash. Flash program too long written to System Log. Issue is seen in automation setups, not likely in customer networks.

Table continues…

Reference number	Description
wi00995011	**7008XLS MDA, Resource Counters**: The “Dropped on no resources” counter does not increment when the ports on the 7008XLS MDA are oversubscribed due to known Unicast traffic.
wi01010266	**Out of Band mgmt port**: Errors display on the console when the OOB mgmt port receives oversized packets.
wi01019793	**IPv6, TFTP**: Binary configuration cannot be retrieved for a stack if using IPv6 management and TFTP server.
wi01028730	**IST**: IST might bounce when a non-base unit rejoins the stack if VLACP short is enabled on IST ports.
wi01029280	**EDM, TACACS password**: If ACLI password type is set to TACACS, Enterprise Device Manager (EDM) is disabled by default.
wi01032538	**Port mirroring**: If you configure all four port mirroring instances, only the first two are functional.
wi01043365	**SMLT, EDM**: Intermittent. Cannot disable or enable IST using EDM (Inconsistent value).
wi01045294	**Stress testing L3**: Stack break might occur In a large configuration with 4k OSFP/RIP routes, 1k VLANs (256 L3 VLANs), and 128k MAC entries.
wi01049115	**Rear port mode, LACP**: LACP mode turned off for rear ports after loading a configuration, when ports are removed from a VLAN.
wi01049203	**EDM off-box**: SNMP agent intermittently times out while configuring or retrieving outputs, IP connectivity is up.
wi01049509	**SMLT LACP**: SMLT LACP bounces at 14k MACs when using LACP Short Timer.
wi01050082	**VCC**: You cannot disable tagging on ports if VLAN configuration control (VCC) is set to automatic.
wi01050158	**EDM off-box**: Timeout occurs when uploading a configuration to TFTP server.
wi01050306	**EDM**: Cannot configure rear ports using EDM.
wi01050558	**EDM off-box**: The default timer cannot be set for VRRP hold-down-timer.
wi01057163	**SNMP**: Timeout when auto saving configuration to NVRAM and performing successive SNMP operations, such as deleting 500 VLANs.
wi01059621	**RADIUS**: RADIUS is not supported on OOB management port.
wi01068140	**VLAN**: Unclear error message if attempting to use VLAN 4001 with SPBM.
wi01090482	**SMLT**: If a Base unit leaves the stack, LAG ports connected to the new Temporary Base unit might intermittently bounce.

Table continues…

Reference number	Description
	Traffic might disrupt if there are no other LACP links connected to other stack units.
wi01100186	**USB**: Console locks when show usb-host-port command is run on the Base unit immediately after a reboot or stack join.
wi01100196	**USB**: Intermittent, USB drive connected to a non base unit might be read after a reboot.
wi01103002	**SMLT/IST over rear-ports**: Traffic might be disturbed for 160 seconds when enabling or disabling VLACP globally in a SMLT configuration.
wi01103345	**AAR/AUR**: Port names are lost after an AAUR or AUR is performed.
wi01103626	**SMLT over rear ports/ASCII configuration**: In an SMLT over rear-port mode configuration, if you retrieve a R10.2 ASCII configuration it might cause an SMLT setup failure in rear-port mode.
wi01105956	**SPBM**: An error might occur when you enable or disable SPBM globally from a non base unit, however the command completes and the stack resets properly.
wi01113745	**Rear-port mode**: If you manually bounce a rear-port with the interfaces shutdown/no shutdown command, one of the rear ports might remain down.
wi01113746	**Rear-port mode**: Intermittent, when you add a Fiber FI cable between two VSP 7000 units in rear-port mode, one of the interfaces might not link.
wi01142492	**SPBM**: SPBM enabled without autosave enabled will not be saved. The switch now verifies if autosave is enabled before it enables SPBM. If autosave is disabled, the switch displays an error to prompt the user to enable autosave before enabling SPBM.
wi01157072	**1 Gbps interfaces**: Unable to disable auto negotiation. Users can now disable auto negotiation on 1 Gbps interfaces to support older products such as the ERS 470 where auto negotiation is unsupported.
wi01115480	**CFM**: CFM does not work on the secondary BVLAN with IPFIX enabled after a stack reset.
wi01115804	**EDM**: SPBM nick names table displays nick-names of 0.00.00 for multiple entries for systems with multiple LSPs.

Chapter 5: Known issues and limitations

Use the information in this section to learn more about known issues and limitations.

Where appropriate, use workarounds provided for the known issues.

Known issues

The following table lists and describes known issues and limitations for Avaya Virtual Services Platform 7000 series Release 10.4. Where available and appropriate, workarounds are provided.

Reference number	Description
wi01229816	Rear port mode SPB: if port 39 goes down, the far end QSFP may bounce port 38.
wi01230409	RMON: DUT doesn't display history records for periodic statistical samples when custom history entry is used.
wi01230454	T-UNI : 802.1q header stripped for half traffic on DMLT after loading up ASCII config
wi01230519	SSH connection error when using RADIUS auth with an username having more than 17 characters
wi01230164	Intermittent: "NVR call to cdt api function failed due to lock timeout" critical message in logs if reboot or shut/no shut all ports of SMLT aggregation DUT.
wi01228907	FA standalone proxy,LACP: fa uplink trunk line fails when config is downloaded and ports are not aggregated into trunk.
wi01228881	FA,LACP: port from TBU gets disabled after TBU reboot.
wi01228926	NEW:FA: LAG ports are disabled after BU power-cycle.
wi01229128	Auto: port mirroring monitor port enables vlan filter-unregistered-frames.
wi01228729	SNMP notification for bsnLoginFailure is disabled after boot default.
wi01228560	Can set TCP port 6000 as SSH port. After SMLT aggregation DUT reboot IST does not come up.
wi01228457	filter-unregistered-frames disable on a TUNI port is not applied properly on a port but present in running config.

Table continues…

Reference number	Description
wi01228440	Intermittent SMLT scaling: #shut/no shut on all ports may not bring up all the interfaces. **Workaround:** C11(config-if)#no shutdown port 3/27,3/30-32,4/ALL %Inactive MDA ports were not enabled.
wi01228013	NEW:SLPP-guard is reenabled on one LACP port if one unit is reset (with other lacp member).
wi01227896	NEW:FA: Incorrect LAG id is displayed by FA elements.
wi01227698	The static MACs configured on SMLT/SLAG are not saved into the running-config.
wi01227161	The console hangs for 270-350 seconds if shut/no shut all ports on SMLT aggr stack with MC and L3 system traffic running.
wi01226566	VSP7000 : Cannot perform Web Login after enabling tacacs. **Workaround:** Either disable tacacs to use EDM or access the switch via telnet.
wi01226499	Dut ip address can not be set from install menu.
wi01226235	Bogus SMLT messages in logs after aggregation stack renumbering: stp group 1 is enable on SLT-unit 0, port X.
wi01226223	It takes ~100sec for rear ports to come up after replacing DAC stack cable with FO stack cable.
wi01226182	FA: uplink lacp BU ports have lacp off when lacp mode off command is issued, even if Cannot modify settings errror is returned.
wi01225837	IST down and traffic does not recover after reboot a SMLT peer with SLPP enabled on multiple SMLTs. **Workaround:** • Have to stop all the traffic. • Reboot the peers to get out from the above state.

wi01225670	When SMLT peer re-joins the cluster MC traffic is causing high CPU utilisation=>VLACP bounces=>210-220sec traffic loss.
	Workaround:
	`C11(config)#interface ethernet all`
	`C11(config-if)#shutdown port 4/13-14,4/17-18,4/7,4/11`
	`C11(config-if)#no shutdown port 4/13-14,4/17-18,4/7,4/11`

wi01225581	AUTO: Ambiguous message displayed when try to enable MAC security on a DMLT with members missing due to stack unit down.
wi01224953	The traffic does not recover via square SMLT core with scaled system traffic running after reboot one SMLT peer.
wi01224940	'#boot secondary default' does not clear the In-band and out-band IP settings.
wi01222119	When base unit resets, All IST/SMLT/SLT links go down until temp base unit takes over.

Table continues…

Reference number	Description

wi01221641	SMLT rear-port mode normal: Copper rear ports links may not come up after upgrade(port bounce solves the problem).
	Workaround:
	`T2(config-if)#shutdown port 38-40`
	`T2(config-if)#no shutdown port 38-40`

wi01221104	Console hangs for about 25 seconds when trying to delete 1k vlans.
wi01220113	EDM: Secondary Flash line is no longer present in EDM.
wi01219149	Can't undo from CLI the MLT istMLT setting that was done from EDM. **Workaround:** Looks like even though the IST setting was removed from CLI the EDM still displays the MLT1 as istMLT. Remove the istMLT setting from EDm in order to modify the MLT settings.
wi01219027	FCoE:fcoe profile applied from EDM/offbox EDM is not saved in confing.
wi01219022	CLIP source interfaces aren`t correctly used for SNMP Traps after globally disable/enable OSPF.
wi01216132	The speed & flow control settings are not kept on 40G MDA ports after upgrade 10.3.3 to 10.4.
wi01214505	MC traffic is briefly filtered when the server starts transmitting even though all the groups are learned on DUT.
wi01213576	NEW_SNMP:Manual: The 40Gig port does not come up if use Avaya 40G-SR4 QSFP VendorPart# JQPR04SWD8AY2.
wi01207227	SPB-scaled QoS Buffering is not kept after partially default a DUT in SPBM mode.
wi01199668	RSTP/MSTP rear ports: The root path cost is the same (200) for MLT/LAGs composed of 3-8 rear ports.
wi01199293	EDM:Sflow: en error is returned when changing MaximumDatagramSize for a configured collector. **Workaround:** Change it from CLI.
wi01199085	SNMP traps are not sent according to the defined source-ip.
wi01198565	EDM: misleading UI behavior when enabling Jumbo Frames.
wi01198335	After stack reset debug messages are displayed in console on units where QQ and XLS MDAs are connected.
wi01197971	If IST is enabled prior of SPBM on the mlt -> PVID is not set to PRIMARY B-VID.
wi01197748	rcIsisPlsbMcastFibOutgoingPorts MIB has value of H when there should be no outport for that multicast-fib entry.
wi01192860	QoS: max burst-size should be selected when not specifying max-burst-duration.
wi01192851	COM 3.1/EDM off-box request timed out error while walking the entire MIB tree, works on EDM onbox.

Table continues…

Reference number	Description
wi01191819	Can set from EDM LossLess mode with any queue-set type.
wi01191739	Not enough HW resources are available. Message appears when configuring a fourth port-mirroring instance, specific config.
wi01190800	Incorrect DHCP enable behavior when there are no HW resources available with meters. **Workaround:** DHCP relay disable -> boot -> DHCP relay enable.
wi01190583	TFTP server IP address not saved/restored from USB binary config.
wi01190335	EDM: 40 Gbps options needed for Traffic Profile Classifier and Set (uniform and individual metering).
wi01190317	CLI Quick start: Cannot configure mgmt ip and netmask using install menu after stack renumbering.
wi01189931	AUTO: the password aging-time setting is not saved across an upgrade from 10.2.x to 10.3.3.
wi01188584	RADIUS+EDM: When using an username with more than 16 characters to connect through EDM, the DUT will not send radius access-requests.
wi01178380	I-SID setting lost after replace XLS MDA with QQ MDA; If try to reconfigure the command fails with "internal error" message.
wi01178224	EDM: missing options to default auto-negotiation advertisements and flowcontrol on interfaces, very useful when making changes and needing to revert, CLI has this.
wi01177050	Connect 7002QQ-MDA to VSP: "Unit needs to be rebooted for MDA to be operational" message NOT displayed if try to enable MDA from EDM.
wi01174490	Difficulty adding ports to an IST running SPBM.
wi01172650	The DUT does not use CLIP IP to send Trap messages after reboot.
wi01169750	Can’t access the DUT after downgrade if serial/telnet Radius or TACACS authentication was set-up with CLIP. **Workaround:** In order to access the DUT, use: • Option 1 After downgrade configure on TACACS/Radius server a client that is matching the IP address of the DUT interface that is sending TACACS/Radius packets and the same shared secret as the one configured on DUT. • Option 2 Download back from DIAG the 10.3.2.x image. The DUT keeps the Loopback settings.
wi01165074	CLI/EDM: Should not be able to enable stack-monitor in rear-port mode normal and spbm.
wi01164562	No message “QuickInstall:USB file not entirely executed” in syslog when we assign a wrong management VLAN from the IP.CFG file.

Table continues…

Reference number	Description
wi01163229	Cannot properly clear/default ip dhcp-snooping external save tftp/ filename settings, entry still remains in running-config and show run has unexpected behavior.
wi01162789	BETA - VSP7000 / MDA Hot Swap / disabled MDA ports are automatically re-enabled after hot-swap.
wi01148247	Wrong Trap description in logs if SLPP-guard enabled port is shutdown after receives SLPP packets.
wi01135068	s5CtrNewHotSwap is generated in logg every time after soft reset.
wi01129952	EDM/EDM off-box: Download Image/Diag from USB with no-reset option is not available.
wi01125021	The show isis adjacency display has an extra line in between entries. **Workaround:** Increase the terminal width with the 'term width 120' command.
wi01120577	Can’t change from EDM the fwd-nh policy mode. Have to delete/re-apply the policy from/to L3 interface with new policy mode.
wi01119837	EDM: No option to select rear-ports in EDM => connot configure SMLT, Rate Limit, Brouter, etc.
wi01119637	The VLANs configured on DUT are not displayed in EDM/IP/ Forwarding-nh Interface Policy/Insert/VLAN selection window.
wi01119107	EDM offbox: incorrect error (commitFailed) when trying to download incorrect image/diag (ok in EDM).
wi01115860	LossLess: Disable/re-enable MLT with STP disabled may cause pause frames flood on MLT links that does not stop after it is enabled on both ends. **Workaround:** Shutdown/no-shutdown the MLT ports.
wi01107903	NEW IP Netstat : CLOSED telnet connection (for inexistent IP) appears too long in "show ip netstat" output.
wi01103119	New OSPF/SMLT: Traffic recovers in 50-60 seconds after shutdown 2 aggr DUTs in square setup. **Workaround:** Attaching the running configs from the DUTs in the diagram.
wi01100008	SLAGs ports are shutdown by SLPP after peer reboot/power-cycle. **Workaround:** The issue is as well reproducible if have the SLAGs connected to multiple edges.
wi01098779	Stack is not reachable for 60-70sec via in-band IPv4, v6 interfaces during image upgrade with no-reset option.
wi01094411	New: Static LACP key binding to trunk ID: Intermittent: LACP key binding to trunk ID fails when defaulting a key and re-binding it to the same trunk ID.

Table continues…

Reference number	Description
	Workaround: Disable the former MLT (MLT 50 in our case) and then do the binding.
wi01093428	New: incorrect script 1 status when download using configure network an ascii file that contains custom script 1.
wi01092693	Multiple NVR Audit data initialized (bad checksum) logged after power cycling 8U high stack 2 times.
wi01089898	EDM: Ambigous errors when tring to remove ip address for the management vlan (Tacacs+/Radius authentication configured).
wi01089759	non-BU ports names are lost after upgrade from 10.2.0.007 to 10.3.0.51 image.
wi01082936	EDM multiple port: cannot set AdminSpeed for multiple selected ports, MDA XT used, works if port is individually selected **Workaround:** Select each port and change it's AdminSpeed individually.
wi01081704	When 10G port 1/1 sends 2 interleaved streams: P0 traffic to 1G receiver and P3 traffic to 10G receiver, P3 traffic is paused at 1G.
wi01079738	EDM - ScriptIndex 1 moves between the 127 rows available in the Ascii Config Script File tab.
wi01074941	Auto: LLDP: Not all tx-tlv options are re-enabled after being disabled/ enabled on all ports when autosave enabled.
wi01068140	VSP7000 R10.2 Trials: Unclear error message when trying to use VLAN 4001.
wi01067876	CFM does not work after reset when ISIS is configured on lower numbered ports and IPFIX is configured. **Workaround:** Disable IPFIX if possible and reset.
wi01066060	SMLT/LACP:A two-link LAG will discard traffic if lacp is set to off on one of them on edge device.
wi01065901	Intermitent : L3 interface is removed from hardware (see error messages and supplemental data).
wi01061676	RADIUS Accounting packets sent even if authentication method is set to TACACS+.
wi01061598	[AUTO]: RADIUS Acct port is not defaulted at "default radius-server" cmd.
wi01058312	Need an explicit error message when try to set mgmt IP and OOB IP from the same class.
wi01058112	Tacacs+: Different syslog messages while connecting through Telnet/SSH with the same username.
wi01051416	MAC address table : After flushing the MAC table and injecting MAC addresses again, the "show mac-address-table" command displays only a few MAC entries, when issued repeatedly.

Table continues…

Reference number	Description
wi01050413	Loading of ASCII config using COM/EDM offbox is inconsistent with config file.
wi01050409	A ping issued to in-band address will be replied via OOB port if a mgmt route is present.
wi01049802	Stack numbering and Stack Health tabs not present in EDM offbox.
wi01049447	VSP7000 R10.2 Trials: Switch stops responding to SNMP after some time. **Workaround:** Issue command "snmp-server enable" to recover.
wi01048163	Extended PSE TLV should not be available on VSP7000.
wi01046657	TDR : After performing TDR between a stack and a standalone VSP7k, on 10 Gig links, the Skew,Swap and Polarity parameters appear only on standalone.
wi01046312	Unable to create a 100Mbps correct link between a ERS family devices and a VSP device if custom speed is used. **Workaround:** Use auto negotiation advertisements of 100-full.
wi01046311	USB load in boot doesn’t work with QoS lossless enabled.
wi01045943	The custom auto negotiation advertisements are set to default after the MDA is unplugged and plugged back in.
wi01044229	IPFIX : L2 streams are sampled by IPFIX as IGP packets, with false destination and source IP.
wi01044187	Intermittent: IPSG binding table has entries even if DHCP binding table has no entry.
wi01042822	SNMPv3 walk on rcVlan tree is interrupted and tooBig error message is returned by net-snmp tool, scaled 1k vlans config.
wi01040435	SNMPv3 inform messages are sent without authentication or privacy even if users are AuthPriv or Auth only.
wi01036502	Rear-port mode: LACP hashing mode should be set to advance, by default.
wi01031752	Setting out of band IP address from install menu fails with â€śCannot modify settingsâ€ť message.
wi01019107	RxTx PauseFrames, Rx FilteredPkts & Tx DroppedOnNoResources port counters missing in EDM.
wi01018538	RMON event time is uptime regardless other source set for clock.
wi01017755	STP state is not restored to initial state after disabling lacp on a SMLT/ LACP trunk.
wi01016012	A route-map named "detail" cannot be filtered when displaying route-maps.
wi01013492	Editable field overlaps port picker if selected before port picker.
wi01012885	Enabling Rear Port Mode in a stack will boot-partial only the BU and NBUs will have Rear Port Mode enabled with.

Table continues…

Reference number	Description
wi01007931	EDM :Pressing ENTER when PktRxThreshold for SLPP interface is selected pops up port selection window.
wi01005423	QoS: ipv6 next-header matching criteria doesn’t work for optional headers, only for L4 protocol id.
wi00998448	Avaya Virtual Services Platform 7000 Series Installation - Implies Switch comes with Power Supply.
wi00992859	AUTO: Copy and retrieving ascii and binary config doesn't work on older USB sticks like Imation 512MB&1GB.
wi00988047	Collision counters on 10G copper ports should be removed since the Half-Duplex mode is not supported.
wi00987926	VSP7000:VSP7000-Trials: Help page title for “Summer Time Recurring error”.
wi00987884	XrxYtxOrYrxXtx, XrxOrYtx, and XrxYtx port-mirror on a DMLT port mirrors ytx traffic on any port of that DMLT.
wi00985066	VSP7000 R10.1 Trials: Same OID returned two different values.
wi00980352	EDM: Cannot display TCP Listeners for IPv4.
wi00979441	AUTO: Configuration objects change unexpectedly during reset tests.
wi00978672	Link is not established on copper MDA ports if port speed fixed at 100Mbps. **Workaround:** Set ports to auto-negotiate, if possible.
wi00977375	DUT doesn't get it's IP address throuhg DHCP server when dhcp mode is "dhcp-when-needed".
wi00976372	Unknown multicast streams are transmitted on router ports even if Unknown Multicast No-Flood is enabled.
wi00976021	Switch ip address is lost when defaulted unit rejoins the stack.
wi00974874	Option to configure snmp traps per port should not be available (10.2 feature).
wi00974728	Inconsistent logging/traps for VLACP Port status.
wi00973743	IGMP groups are not learned when router-alert is enabled. **Workaround:** Disable router-alert and groups will be learned.
wi00973613	(GDS): Failed to lock NvRam files errors sometimes occur on NBU when resetting stack.
wi00973558	Inconsistency between CLI and EDM related to NotifyControlPortList after one of the NBU is shutdown.
wi00972626	LACP : Spanning tree learning is disabled on LACP ports, in multiple STG configuration scenario.
wi00972073	EDM: The OOB management port is not green in Device Physical View when that port has link.

Table continues…

Reference number	Description
wi00972027	Unified User Auth: password types output doesn’t change when setting the missing ip address
wi00971631	EDM - Down Units are doubled in Device Physical View.
wi00971608	NUQC:DUT doesn't take various settings from quickconfig such as spanning-tree, rate-limit, vlacp.
wi00971555	NUQC:Ports which are set by quickconfig on vlans are erased after AUR is performed.
wi00971049	AUTO: tCliAudit errors writing to flash -- Flash Program too long. **Workaround:** Erase the configuration on the DUT -- going back to a default configuration.
wi00970803	SSH session closed (lost connection) while applying ASCII configuration within the same session. **Workaround:** ASCII configuration is applied ok and session remains active if I remove the fallowing lines in the ASCII file.
wi00968578	High frame loss for each port pair in IxAutomate throughput test for a 2high ring stack, 24 port pairs, no MDA used(not in build 043).
wi00967715	Syslog:Logging/traps are received by syslog server with delay and not in initial order.
wi00965952	LossLess stack: sending rate decreases on clients connected to other unit than the receiver; senders on remote unit will share a lower rate depending on front panel port index.
wi00934578	Cannot interrupt a ping to a host name.
wi00932727	EDM: Can’t add and display MACs in MAC-security DA-filtering table.
wi00908784	Doc: Due to different MLT hash-calc formula traffic loss may occur if connect VSP7k to VSP9k, ERS55xx/56xx.
wi00896020	The “sho mlt hash-calc” command can be executed without entering all values.
wi00884529	Port mirror mode xrxorxtx adds vlan tag to packets for untagged tx mirrored traffic.
wi00882956	SFPs that cannot reside in neighboring slots in the VSP.
wi01186992	IST is not functional if configured on rear ports when using ASCII cfg file. **Workaround**: Reset the Unit after Configuration completed and IST will come up.
wi01190811	Intra-stack communication failure error returned on a 3-high stack when trying to save the binary config to tftp: **Workaround**: Repeat the command and save should complete normally.
wi01192712	LossLess: "(config-if)#default flowcontrol" on all ports in mixed stack does not set flow control to Symmetric on 7024XT ports.

Table continues…

Reference number	Description
	Workaround: Default Specific ports on 7024XT units if needed.
wi01197971	If IST is enabled prior of SPBM on an MLT, PVID is not set to PRIMARY B-VID.
wi01196895	The in-band IP may not be reachable if on sFlow enabled ports send/ receive MC traffic using small frame sizes (68-256) at 40-100% line rate.
wi01196917	The in-band IP may not be reachable if have sflow enabled on multiple interfaces with known unicast traffic running at Line Rate.
wi01158262	Multicast traffic is not forwarded to member ports when running in TBU with multicast-filter-mode enabled.
wi01086050	**Rear-port mode**: Fiber Fabric Interconnect cables are auto-negotiation disabled, so flow control settings show as disabled or asymmetric.
wi00933142	**EDM, MLT BPDU setting**: When using Enterprise Device Manager (EDM), it is not possible to specify the MLT BPDU send or receive mode settings.
wi01127831	**VLACP**: VLACP may bounce under high CPU usage.
wi01179263	LACP is flapping on SLT/SLAG ports if download image no-reset (~120 sec traffic loss). VLACP may NOT come up on some of the SLT/SLAG ports after download.
wi01167272	Starting with SW 10.3.3, LLDP MED TLVs will not be sent between units although MED TLVs are enabled. Show lldp neighbor med will not display MED information.
wi01179822	OSPF Full Mesh support needs to be documented a little better per customer recommendation.
wi01187218	Dropped on no resources packets are not captured by sflow sampling in lossless mode with flowcontrol asymmetric.
wi01188232	If the unit is used in many to one lossless scenario, enabling sflow at high sampling rates on Tx ports can affect the throughput at the Rx port.
wi01187359	QoS drop or meter on ingress does not influence sflow ingress sampling. QoS shaper on egress does not influence sflow egress sampling.
wi01186368	All sflow samples appear as tagged.
-	When a SCB profile is applied for a group or a range of groups, IGMPv3 reports are dropped, but sflow samples incoming IGMPv3 reports for those groups.
wi01187751	Egress packets that are dropped on no resources are captured by sflow egress sampling although such packets do not exit from DUT.
wi01185394	Sflow: malformed datagrams for a specific buffer size of "3000" may be seen via Collector. All other sizes are correct.
wi01186351	(CVLAN) samples that still have mac-in-mac encapsulation are collected.

Table continues…

Reference number	Description
wi01187191	In case of using sflow and "Unicast Storm Control/multicast-filter-mode" the sflow application forwards samples to the collector even for dropped packets.
wi01187826	For ingress packets: Packets are sampled (seen on SFLOW) whether mac security is enabled or disabled. For egress packets: Packets are sampled only when mac security is disabled.
wi01191608	Sflow: egress flow samples have input interface 0 when traffic is ingressing an MLT.
wi01177501	If RW username was modified in a prior release it is reset to "RW" (after upgrading to 10.3.2). **Workaround**: Working as Designed. In this feature we are not allowed to change the user's name. Once you create a user it stays with that name until it is deleted. The default users are named RW and RO and we cannot change their names.
wi01183598	SLAMon Agent Registration fails if server is reachable using mgmt i-sid over NNI ports. **Workaround**: None
wi01181004	SMLT over LACP - ports with LACP timeout set to short, may intermittently filter traffic. **Workaround**: Set LACP timers to Long. **Note:** Avaya recommends when configuring LACP over SMLT, LACP Long timers are used.
wi00972139	**AAUR/DAUR, Release 10.0**: If you add a VSP 7000 switch running a software release prior to 10.1 to an operational Fabric Interconnect Stack, the unit will not join the stack. The UP/Down LEDs will remain amber on the 10.0 switch to indicate that the unit is unable to correctly join the Fabric Interconnect Stack. **Workaround**: You need to upgrade the agent code software on a VSP 7000 to release 10.1 or later before adding the unit to an operational Fabric Interconnect Stack.
wi00978314	**EDM, 32 ports**: When using Enterprise Device Manager (EDM) with the VSP 7000, some work areas might incorrectly indicate 32 ports are present, even if no MDA is or has been inserted in the switch.
wi00949421	**EDM, Chrome**: If you use Google Chrome to access the switch via Enterprise Device Manager (EDM), then you might not be able to login to the switch if local username and passwords are configured.

Table continues…

Reference number	Description
	Workaround: The supported browsers for managing a VSP 7000 switch are IE or Firefox. It is recommended to use one of the supported browsers.
wi00971757	**Lossless Mode**: When the switch is operating in Lossless mode and flowcontrol is disabled on a port, the dropped on no resources counter stays at zero on egress port, even if the port becomes over-subscribed. **Workaround**: You must enable flow control on all ports if the switch is operating in Lossless mode.
wi00974573	**LACP**: LAGs might show duplicates on a Temporary Base Unit when you perform `show lacp agg`. **Workaround**: LAGs are not duplicated, this is a display issue only.
wi01048943	**Port mirroring**: ManytoOneRxTx port mirroring instance does not work for unknown unicast, multicast, and broadcast traffic.
wi01053545	**LACP/SMLT**: When a unit with a LAG port rejoins a stack, there might be packet loss or flooding for up to 25 seconds.
wi01066446	**Rear-port mode**: If you change between standard rear-port mode and SPB rear-port mode the switch requires a reboot and partial configuration reset. Standard rear-port mode does not support SPB.
wi01011829	**VRRP**: Intermittent. Error message might occur when enabling or disabling VRRP. **Workaround**: Reset the unit.
wi01018227	**EDM**: If an active 10 Gb copper interface is enabled using EDM, the port status is amber although the port is up.
wi01026033	**OOB MGMT**: Autotopology is not functional on the Out-of-band management interface
wi01034248	**Rear-port mode**: Port 40 linked to port 36 in rear-port spb mode can cause inconsistency regarding port state. **Workaround**: This is an invalid configuration.
wi01046994	**EDM, LLDP**: LLDP tx-tlv local-mgmt-address disables on all MDA ports if disabled on one port. **Workaround**: Use ACLI to re-enable the TLVs disabled on the MDA port. **No Fix Planned**
wi01048843	**Rear-port mode**: Binary configuration of a unit with rear port mode enabled cannot be retrieved on a defaulted unit.
wi01061172	**EDM off-box**: Using Element Manager authenticated with SNMPv3 cannot create additional SNMPv3 users and causes error messages. **Workaround**: Use EDM on-box or ACLI to configure.
wi01064985	**EDM off-box**: Packet per second (PPS) rate limit value cannot be defaulted (0), timeout.

Table continues…

Reference number	Description
	Workaround: Use EDM on-box or ACLI to configure.
wi01050783	**SLPP**: LACP SLT links are disabled without loops after reboot with aggressive values 5 and 50. **Workaround**: Configure the threshold values at least 5 times the number of VLANs and use long timers.
wi01050967	**EDM**: IP ARP tab cannot display the brouter static ARPs if the ARP table contains multiple entries. **Workaround**: Use ACLI to display the table.
wi01052477	**EDM**: EDM multiple port configuration mode cannot configure the speed on multiple MDA ports. **Workaround**: Modify a single port at a time or use ACLI to modify multiple ports.
wi01017515	**EDM**: The asset ID string that follows after a < character does not display in EDM. **Workaround**: Use ACLI if required
wi01057995	**Show port** : Enhancement info is incomplete when issuing show port over SSH with a terminal length of 0. **Workaround**: Configure the terminal length to 40 and try again.
wi01060852	**RADIUS**: You cannot use EDM to change the RADIUS password. **Workaround**: Use ACLI to change the password.
wi01061771	**Display**: 50 m and 100 m fiber rear port connections show as 0.0m length with show stack-cable command.
wi01062498	**SMLT**: An error does not display when peer IP is the same as the local VLAN IP.
wi01068432	**SPBM**: SPBM nickname starting with 3.33.33 causes Multicast traffic to drop. **Workaround**: Do not use SPBM nicknames that begin with the string 3.33.33. Other nicknames are not affected.
wi01089619	**Stress testing PFC-lite**: Stack of 8 in lossless-pfc mode, with 8 to 1 oversubscription might break the stack after a unit reboots.
wi01094873	**EDM**: The **Single Port SMLT** tab might show duplicate SLTs. This is a display issue only.
wi01093829	**Scaling SPB**: High CPU utilization might occur if you configure SPBM with over 800 CVLANs on a switch or stack. **Workaround**: Avaya recommends a configuration below 800 CVLANs.
wi01111498	**Scaling SPB**: IS-IS adjacency continuously bounces after a port with 145 nodes/2500 i-sids is manually bounced on a stack with VLACP enabled.

Table continues…

Reference number	Description
wi01108966	**EDM**: Toggling between L2TraceRoute and L2TraceTree does not work after the first attempt. **Workaround**: Repeat the command, the second attempt should be successful.
wi01101710	**IPFIX/SPB**: IPFIX does not sample data on SPBM ports when traffic passes through to another port.
wi01093185	**SPB**: Port mirroring mode xrxorxtx sends 2 packets for each packet received by the UNI mirrored port. One Tagged and one Untagged packet is sent and can disrupt multicast, broadcast, and unknown unicast traffic. It should not impact known unicast traffic. This issue was found in the following configuration: Mirrored port is a single untagged port in a CVLAN and ingress traffic is untagged. The mirroring port is untagged. The mirrored traffic shows one untagged packet and one tagged packet (PVID on port for VLAN tag).
wi01092396	**RIP over SMLT**: After a unit re-joins the SMLT cluster, traffic loss might occur for 72–96 seconds.
wi01119196	**LACP/Transparent UNI**: LACP does not work on Transparent UNI ports. **Workaround**: None - LACP is not supported with Transparent unit.
wi01119204	**Transparent UNI**: Transparent UNI does not add other ports of the same LAG if the partner is down.
wi01122829	**EDM**: When you configure Rate Limit, if you enter a value for the **AllowedRatePps** field for multicast only, even if this is disabled , in ACLI that pps value is set for broadcast also, which is enabled on EDM. **Workaround**: Use ACLI when you configure this mode.
wi01087988	**EDM multiport**: Multicast/broadcast is not set accordingly in a 3 unit stack when you apply the configuration on all ports besides mgmt. **Workaround**: Use ACLI to configure.
wi01094742	**Automation**: Port names on non base units may be lost after upgrade from 10.2 official release to 10.3. **Workaround**: None
wi01011165	**EDM**: When booting the device in Rear-Port mode the configuration is not partially defaulted. **Workaround**: Use ACLI when you place a unit in Rear-Port Mode.
wi01051679	**LACP**: LAG replaced by MLT in configuration after power-cycle. This is a very intermittent issue. **Workaround**: Seems to be a display issue only. LACP PDUs still transmitted and received. After another reset will go back to being displayed as AGG.

Table continues…

Reference number	Description
wi01062821	**Port mirroring**: Port mirror strips 802.1ah header from SPBM encapsulated control packets. **Workaround**: None
wi01079180	**EDM**: BlinkLEDs is not functional in EDM. **Workaround**: Use ACLI if you need to use the **`blink-leds`** command to discover a unit.
wi01092850	**EDM**: Minimum burst size (2 Kbytes) cannot be created for QoS interface shaper. **Workaround**: Use ACLI to modify.
wi01095355	**EDM**: IPv6 Tunneling: Can delete IPv6 manual unicast address for a tunnel interface but there is no easy way to add it back. **Workaround**: Use ACLI to remove.
wi01103646	**EDM**: Changes needed for QoS metering with high committed rates .When using high committed rates for QoS meters and if-shapers (above 2 Gbps), use higher burst-sizes. Lowest burst-sizes are not supported for high committed-rates (above 2 Gbps). Such configuration is not allowed in ACLI, but is allowed in EDM and may produce lower traffic rates than expected. **Workaround**: Configurations can be done correctly in ACLI.
wi01113078	**EDM**: Device continues to filter traffic even if ports are included in SecurityLockoutPortList via EDM. **Workaround**: Use ACLI to configure.
wi01116249	**EDM**: When creating a new MSTP MSTI instance you need to manually refresh the tab to see the instance.
wi01117878	**EDM/IPv6 OOB**: Incorrect information for IPv6 neighbors is learned over the OOB interface. **Workaround**: Use ACLI to view this information.
wi01122650	**L2/LACP based SMLT**: Full traffic recovery takes 30 seconds when an NBU rejoins the stack. **Workaround**: None - Optimization of LACP may occur in future release.
wi01098825	**VRRP/LACP over SMLT**: Up to 30 seconds traffic loss when BU of aggregation SMLT device in the data path leaves the stack or ex-BU re-joins the stack.
wi01132657	**Stack cable**: If a fiber or copper stack-cable is inserted after agent initialization, Stack-cable-info is Not Available.
wi01132658	**Stack cable**: Stack-cable-info is not updated when you swap 100 m fiber cable with 10 m fiber cable (and the reverse).
wi01133274	**SPBM**: May see up to 10-20 second traffic loss for SPBM traffic when the base unit of a stack is reset.

Table continues…

Reference number	Description
wi01151663	**Rear-Port mode**: When downloading a binary configuration to a unit that was in Rear-Port mode, the download can fail. **Workaround**: Place the unit in Rear-Port mode prior to starting the binary download.
wi01089213	**EDM**: There is no option in EDM to set the port speed for out-of-band management. **Workaround**: Use ACLI to configure.
—	When using fiber FI cables in rear-port mode, intermittently, one or more of the 40 Gbps links may not obtain link after a switch upgrade or peer reset. Verify the link status of ports 33 to 40 if running in rear-port mode and a reset has occurred. The link can usually be disabled and re-enabled with the **`shutdown`** and **`no shutdown`** commands from the ACLI.
wi01125492	**Layer 3/SMLT with OSPF**: Traffic downtime of 40 seconds or more when SMLT peer comes back up; unexpected in this specific configuration and scenario. **Workaround**: Use MLTs instead of LACP for faster recovery. Consider an OSPF over SMLT triangle configuration, using LACP as the basis for the SMLT. In the event that an SMLT peer device goes down and rejoins the cluster, it is possible to see traffic recovery times upon rejoin of up to 50 seconds. Avaya recommends that you use MLT instead of LACP whenever possible, to minimize the impact of such events.
wi01166124	**SPBM/SMLT**: Trafffic does not forward from a port on one Split BEB to the other split BEB in the same cluster when ISIS cost is not over IST. **Workaround**: The shortest path between the the two split BEBs MUST to go through the IST in order to have all traffic forwarded correctly. NNI cost needs to be configured accordingly.
wi01082141	In-band connectivity to DUT is lost for 25-70 seconds if disable/enable the IST **Workaround**: None - Disabling IST is not recommended.
wi01123256	**IPv6**: Traffic does not recover if the forwarding SMLT aggregation DUT goes down. **Workaround**: None - IPv6 is not supported across SMLTs.
wi01133274	10-20 second traffic loss may be seen for SPBM traffic when the Base Unit of a Stack running SPBM is reset. **Workaround**: None
wi01138707	EDM option to set port speed at 10 Mbps should be grayed out. Should be unable to set this port to 10MB.
wi01160110	EDM should aggregate Trunk based interfaces such as the CLI does **Workaround**: None - Use CLI as needed.

Table continues…

Reference number	Description
wi01163387	**VSP7000 - 10.3.0.0**: Non-QoS application CFM consumes 2x precedence masks limiting use of QoS policies.
wi01169060	**Rear port mode 10M Fiber cable**: Bounce ports 34-35. Port 36 gets bounced as well when no shut command is done. **Workaround**: None - All ports will link back up, minimal traffic loss on failure.
wi01162149	AdminDuplex=Half and AdminSpeed=mbps10 option should NOT be available in EDM. **Workaround**: None - The VSP7024 units DO not support 10MB. Don not attempt to set to 10MB as it is not supported.
wi01142088	SLPP does not bring down the rear-ports if load the ASCII config while a loop is present. If loop is active after the ASCII config is loaded, then SLPP works.
wi01092850	**EDM**: Minimum burst size (2 Kbytes) cannot be created for QoS interface shaper. **Workaround**: Use ACLI to configure.
wi01143415	**SPBM**: QoS meter is not working as expected on unicast that enters NNI and exits UNI. QoS rate problems are due to SPBM encapsulation, or qos matching pattern moved.
wi01143412	**SPBM**: QoS shaper is not working as expected on broadcast that enters NNI and exits UNI. QoS rate problems are due to SPBM encapsulation, or qos matching pattern moved.
wi01143418	**SPBM**: QoS does not match ip-elements on traffic that enters NNI and exits UNI. QoS rate problems are due to SPBM encapsulation, or qos matching pattern moved.
wi01162309	**SPBM/EDM**: User can Delete IS-IS Manual Area leading to adjacencies loss. - This should be blocked or a message displayed alerting user of potential mistake.
wi01167267	QoS buffering does not get changed to SPB-scaled when rear-port mode spbm is enabled. **Workaround**: A second reset is required to enable this buffering setting after making modification.
wi01162268	**SPBM**: Transparent i-sid can be configured for LACP enabled ports which can lead to inconsitency in stack. **Workaround**: None - LACP is not supported with Transparent Uni and should be blocked.
wi01117324	The **`show clock detail`** command displays NTP time without time zone. There is an inconsistency between SNTP time and NTP time in **`show clock detail`**. For SNTP, time is displayed as GMT+time zone and for NTP time, only GMT is displayed.

Table continues…

Reference number	Description
wi01125492	**L3/SMLT with OSPF and LACP**: traffic downtime of 40 seconds or more when SMLT peer comes back up. **Workaround**: Use regular MLT in this situation instead of LACP.
wi01103323	**L3/SLAG of 4**: Traffic does not recover if power off on edge stack a unit that has 2 of the 4 LAG up-links. In this particular scenario, when the one of the two unit of the edge is powered off, the LACP will de-aggregate and the protocol will be restarted. Since only 1 link remains up on each core device, we are ending up in a situation equal to the one when we try to configure from the beginning SMLT over LACP using only 2 links. When we try from the beginning to configure a SMLT over LACP with only 2 links, one on every core, on the edge we have two links, enough for the LACP to aggregate, but because on the cores only one link is configured as LACP it will not aggregate. In this situation, the SMLT prevents the LACP from using the configured smlt-sys-id, and LACP sends messages with the default sys-id until at least 2 links are up or the MLT is aggregated on the cores. Due to this, the LACP will not aggregate on the edge. Because the ports are configured on SMLT and LACP port-mode is *advance*, the ports will remain in blocking to prevent a loop.
wi01147278	SPBM/SMLT: MAC-security does not work on CVLANs on 7ks with SMLT enabled. **Workaround**: Mac Security should work on ports other than MLTs/ LACPs. Not yet supported on Trunks on the VSP7K.
wi01068125	Up to 4sec packet loss when performing SMLT link failover to ERS8800 in a Square topology.
wi01078780	VSP7000 R10.2 Trials: Unable to see rear ports in EDM.
wi01105678	PC still has network access after removing its MAC from SecurityTable using: #no mac-security mac-address-table mlt-id. **Workaround**: Access will be dropped with in 1-2 minutes of removal.
wi01118514	Radius use-management-ip : DUT doesn't use management ip in forced stack mode. **Workaround**: None
wi01121109	Unicast Storm Control: Fail to apply NQ policy on a port that has other QoS policies. **Workaround**: Remove QOS Policy for specified port.
wi01130872	bsnSFP Insertion/Removal Traps and Log Message regarding Vendor and Transceiver Type should be sent to Trap/Log receivers for rear ports.
wi01132496	Request Time Out! message is displayed when Disable/Enable IST from EDM off-box.

Table continues…

Reference number	Description
	Workaround: Use ACLI in this case.
wi01163385	Traffic is not forwarded to the IP fwd-NextHop if have configured static ARP for the NH.
wi01163754	SMLT scaling: 13 seconds recovery time for L3 traffic when power-cycling IST peer Large scaled environment.
wi01168418	EDM off-box/Edit/Chassis/Switch/Stack: StackNumbering & StackHealth Tabs are missing. **Workaround**: Use ACLI to configure/monitor.
wi01170038	MLT utilization is not displaying the expected value when using QQ MDA Ports at maximum bandwidth the MLT is up but Utilization displayed at incorrect value. **Workaround**: None at this time.
wi01172124	Cannot download image/diag using stack OOB IP if the console is connected to non-Bus.
wi01177630	40Gig port LEDs are not functional on port shutdown and on blink-LEDs unless there is a QSFP connected to the port.
wi01179084	If unit contains a 40G MDA and is in Rear Port Mode. Link Led on port 7 may be on even though Link is not present.
wi01179683	Lossless/PFC: LAG does not form after OFF/Active with STP disabled(LACP port-mode=advanced).
wi01083838	EDM: Cannot set Console Password Type "Tacacs Authentication". **Workaround**: Use ACLI.
wi01171533	EDM could return authentication failed when retrying EDM login with correct credentials and lockout time expired, if previous login attempts locked the user. EDM can be safely accessed after that if pressing return to login page.
wi01157075	**SPBM over SMLT**: Intermittent issues with SPBM over SMLT occur if you filter untagged frames on the IST. **Workaround**: When running SPBM over SMLT, make the PVID of all IST ports the primary B-VLAN, and do not enable Filter-Untagged-Frames on IST ports.

Limitations

The following sections provide information about limitations and assumptions for Software Release 10.3.3.

sFlow limitations

The following table lists sFlow specific limitations.

Description	Status
SFlow Configuration Limitations	
maximum number of configurable sFlow collectors	4
sFlow sample size	64-256 bytes
sFlow collector delete timer configuration range	0-65535 seconds
sFlow collector buffer size	400-9216 bytes
sFlow sample rate range	4096-1000000
sFlow port counter interval	1-3600 seconds
Sflow Unconfigurable Limitations	
sFlow vlan counter interval	Hardcoded to 30 seconds, the sFlow vlan statistics are enabled when sFlow is globally enabled.
Sflow can be enabled only on front panel ports	
Sflow Hardware Limitations based on ASIC capabilities	
sFlow vlan statistics	Cannot capture specific vlan statistics for unicast/multicast/broadcast/ discard packets. Only the total number of bytes sent or received in a vlan is available.
Since the sflow sampling is done for both ingress and egress on the ingress pipe, the information regarding the destination port is unavailable at this level for all types of packets.	For ingress samples, the source id class and index are the ingress port in ifIndex format. For egress samples, the source id class and index are equal to: • 0 (meaning unknown) for unicast. • The egress vlan id for multicast and broadcast (in vlan format) Assumptions: • Egress samples are sent to all configured collectors. • Sample rate is set to 0 (You cannot check the value for unknown interfaces for a specific vlan). • Egress samples use the same sequence number variable. • Sample length have the default value set to 124 bytes. • Sample pool is always 1. • Dropped value is always 0.

Filter resource consumption

Applications consume filter resources, which are a combination of masks and filters, also known as rules.

A filter specifies the bit pattern to match. A mask specifies the bit position to match and the evaluation precedence of the filters.

The following table summarizes the applications that require mask and filter resources. The values are per port.

Table 1: Application mask and filter resource requirements

Application	Category	Symbol	Masks required	Filters required	Meters required
Broadcast ARP (precedence 10)	Non QoS	AR	1	1	Yes
DHCP Relay or DHCP Snooping	Non QoS	DH	1	4	Yes
QoS interface group (untrusted and untrustedv4v6)	QoS	Q	2	2	No
One QoS policy	QoS	Q	1	up to 200 if blocks are used	Yes / No
One QoS traffic profile set	QoS	Q	up to 8	up to 75 if blocks are used	Yes / No
Port Mirroring (MAC-based or XY)	Non QoS	PM	1	2	No
IPFIX	Non QoS	IF	1	1	Yes
RIP	Non QoS	RI	1	1	No
VRRP or OSPF	Non QoS	DR	1	1	No
UDP Broadcast	Non QoS	UB	1	1	Yes
IP Source Guard	Non QoS	IS	1	11	No
FCoE redirect	Non QoS	FC	3 or 4	3 for first profile and another 1 for each profile	No
SPBM	Non QoS	SB	1	1	No
Mac security DA filtering (Bay Secure)	Non QoS	BS	1	1 for each MAC address	No
Content-based forward to next hop	Non QoS	CF	1 for each CF policy applied per port	1 for each mask	No
CFM	Non QoS	CM	2	1 for each mask	No

Table continues…

Application	Category	Symbol	Masks required	Filters required	Meters required
SLPP Guard	Non QoS	SP	1	1	Yes
IGMP snooping	Non QoS	MC	1	2 for first vlan and another 1 for each vlan	Yes
DHCP SPBM	Non QoS	DS	1	6 per unit	Yes

Important:

If Filter Manager resources are not available after an upgrade, the following features cannot be configured:

- DHCP Relay or DHCP Snooping
- QoS
- Port Mirroring
- IPFIX
- RIP
- VRRP or OSPF
- UDP Broadcast
- IP Source Guard
- FCoE redirect
- MAC security DA filtering (Bay Secure)
- Content-based forward to next hop
- SLPP Guard
- IGMP snooping

Virtual Services Platform 7000 Series shares resources across groups of ports (ASIC). Each group of ports has the following available resources:

- 10 masks
- 256 filters for each mask (precedences from 5 to 10)
- 128 filters for each mask (precedences from 1 to 4)

By default, the system consumes the following:

- one mask (precedence 10) and one filter for ARP filtering on all ports
- one mask (precedence 9) and one filter for SPBM on all ports
- one mask (precedence 8) and three filters for DHCP on all ports

You can use the **`no ip dhcp-relay`** command to free precedence 8 (DHCP). You cannot free precedences 9 and 10, which leaves 8 available masks for each group of ports for QoS and non QoS applications to configure dynamically.

Each group of ports has 128 meters available for each mask. The system can use meters in a maximum of four precedences per ASIC (QoS and non QoS meters).

Each group of ports has a maximum of 128 counters or track statistics (precedences from 5 to 10), and a maximum of 64 counters (precedences from 1 to 4). Each group of ports has a maximum of 32 QoS range checkers.

Note:

The system can use meters in a maximum of four precedences for each ASIC (QoS and non QoS meters). If precedence with meters is not available, the value for *Meter Total* is displayed as 0 in **`show qos diag`**. When upgrading, features that require extra resources can get disabled if there is no space for precedences or precedences with meter.

Masks and filters inventory check

You can use the **`show qos diag`** command to assess the current filter resource usage for each port. The **`show qos diag`** command displays the number of QoS masks and filters and non QoS masks and filters that each port consumes. You can determine whether you can enable an application that requires filter resources on a port by verifying that the number of available masks and filters meets the mask and filter requirements of that particular application.

Note:

It is recommended to configure QoS after all the features are configured.

Use the output of the **`show qos diag`** command to count the unused masks to determine the number of available masks for a particular port. The filters that QoS or non QoS applications use on a port for a specific mask determines the available filters for that mask for all ports from that group.

You can determine the number of the filters available for a mask from a group of ports by adding the total number of QoS and non QoS filters in use and subtracting that number from 256 (or 128). If the number of filters in use for a mask is equal to 256 (or 128), you cannot use that mask on other ports from the same group.

The following example illustrates this process for the IP Source Guard application.

To enable IP Source Guard on a port requires 1 mask and 11 filters. To verify that you can enable IP Source Guard on port 5, you can view the following **`show qos diag`** output and determine that port 5 is currently using a total of 3 masks (non QoS). IP Source Guard uses the next available mask and from the output, you can see that there are 256 filters available for mask 7, which meets the IP Source Guard requirement of 1 mask and 11 filters.

```
7024XLS#show qos diag


Unit/Port           Mask Precedence Usage
          10   9   8   7   6   5   4   3   2   1
--------- ----------------------------------------
1/1        AR  SB  DH
1/2        AR  SB  DH
1/3        AR  SB  DH
1/4        AR  SB  DH
1/5        AR  SB  DH
1/6        AR  SB  DH
1/7        AR  SB  DH
1/8        AR  SB  DH
1/9        AR  SB  DH
1/10       AR  SB  DH
1/11       AR  SB  DH
1/12       AR  SB  DH
1/13       AR  SB  DH
1/14       AR  SB  DH
```

```
1/15         AR  SB  DH
1/16         AR  SB  DH
1/17         AR  SB  DH
1/18         AR  SB  DH
1/19         AR  SB  DH
1/20         AR  SB  DH
1/21         AR  SB  DH
1/22         AR  SB  DH
1/23         AR  SB  DH
1/24         AR  SB  DH
1/25         AR  SB  DH
1/26         AR  SB  DH
1/27         AR  SB  DH
1/28         AR  SB  DH
1/29         AR  SB  DH
1/30         AR  SB  DH
1/31         AR  SB  DH
1/32         AR  SB  DH

AR=ARP DH=DHCP SB=SPB

                                    NonQoS NonQoS
 Unit/Port  Prec Filter Meter Cntr Filter  Meter Filter Meter Cntr  RngChk
                Used  Used  Used  Used    Used  Total  Total Total  Used
----------- ---- ------ ----- ---- ------ ------ ------ ----- ----- ------
1 /1 -32    10   0      0     0    32     32     256    128   128
            9    0      0     0    32     0      256    128   128
            8    0      0     0    96     32     256    128   128
            7    0      0     0    0      0      256    128   128
            6    0      0     0    0      0      256    128   128
            5    0      0     0    0      0      256    128   128
            4    0      0     0    0      0      128    128   64
            3    0      0     5    0      0      128    128   64
            2    0      0     0    0      0      128    128   64
            1    0      0     0    0      0      128    128   64
                                                                0 /32
```

The following output shows the **`show qos diag`** output after you enable IP Source Guard on port 5.

```
7024XLS#show qos diag


Unit/Port           Mask Precedence Usage
           10   9   8   7   6   5   4   3   2   1
--------- ---------------------------------------
1/1          AR  SB  DH
1/2          AR  SB  DH
1/3          AR  SB  DH
1/4          AR  SB  DH
1/5          AR  SB  DH  IS
1/6          AR  SB  DH
1/7          AR  SB  DH
1/8          AR  SB  DH
1/9          AR  SB  DH
1/10         AR  SB  DH
1/11         AR  SB  DH
1/12         AR  SB  DH
1/13         AR  SB  DH
1/14         AR  SB  DH
1/15         AR  SB  DH
1/16         AR  SB  DH
1/17         AR  SB  DH
1/18         AR  SB  DH
1/19         AR  SB  DH
```

```
1/20        AR  SB  DH
1/21        AR  SB  DH
1/22        AR  SB  DH
1/23        AR  SB  DH
1/24        AR  SB  DH
1/25        AR  SB  DH
1/26        AR  SB  DH
1/27        AR  SB  DH
1/28        AR  SB  DH
1/29        AR  SB  DH
1/30        AR  SB  DH
1/31        AR  SB  DH
1/32        AR  SB  DH

AR=ARP DH=DHCP IS=IPSG SB=SPB

                                      NonQoS NonQoS
 Unit/Port  Prec Filter Meter Cntr Filter  Meter Filter Meter Cntr  RngChk
                Used  Used  Used  Used   Used  Total  Total Total  Used
----------- ---- ------ ----- ---- ------ ------ ------ ----- ----- ------
1 /1 -32    10   0      0     0    32     32     256    128   128
            9    0      0     0    32     0      256    128   128
            8    0      0     0    96     32     256    128   128
            7    0      0     0    11     0      256    128   128
            6    0      0     0    0      0      256    128   128
            5    0      0     0    0      0      256    128   128
            4    0      0     0    0      0      128    128   64
            3    0      0     5    0      0      128    128   64
            2    0      0     0    0      0      128    128   64
            1    0      0     0    0      0      128    128   64
                                                                0 /32
```