Release Notes for Avaya Virtual Services Platform 7000 Series

Release 10.3
NN47202-400
Issue 05.02
March 2014

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “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.

Licence types

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

Heritage Nortel Software

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

Copyright

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

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

This document 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

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.

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://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 site.

✱ **Note:**

Videos are not available for all products.

Support

Visit 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

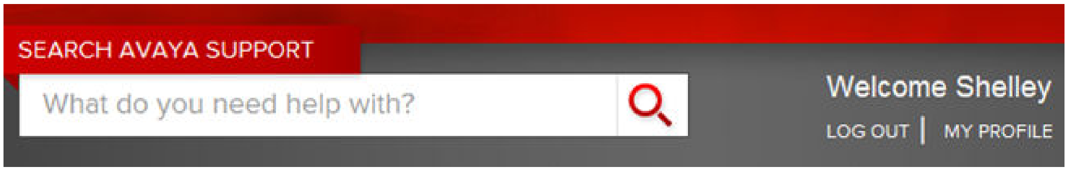
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support web site.

About this task

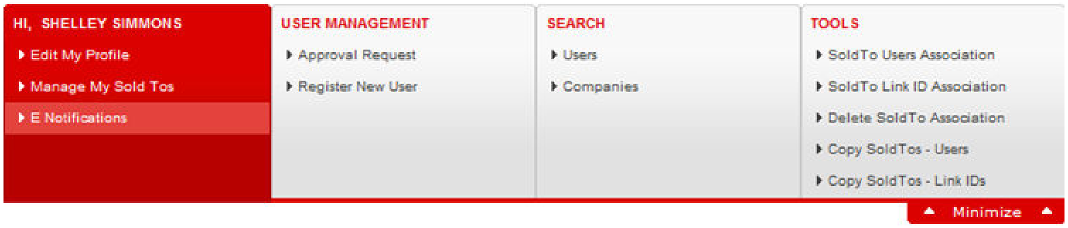
You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), that apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Ethernet Routing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

Procedure

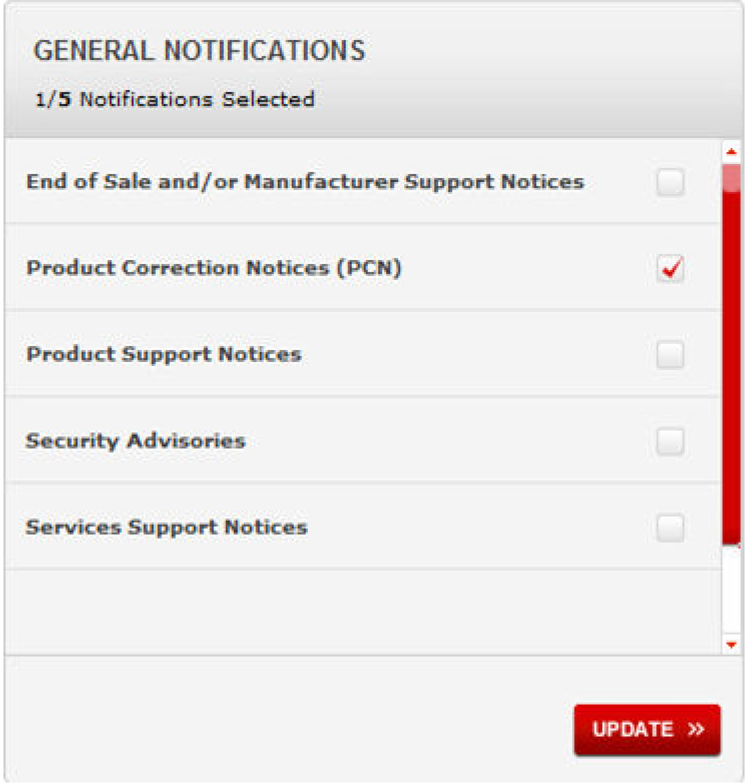
1. In an Internet browser, go to https://support.avaya.com
2. Type your username and password, and then click **LOG IN**.
3. Click **MY PROFILE**.



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



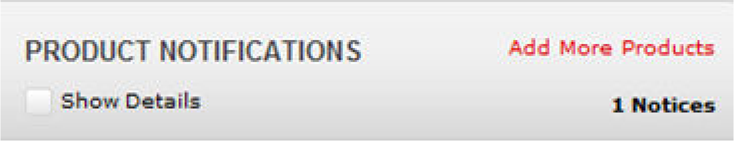
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.


GENERAL NOTIFICATIONS

1/5 Notifications Selected

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

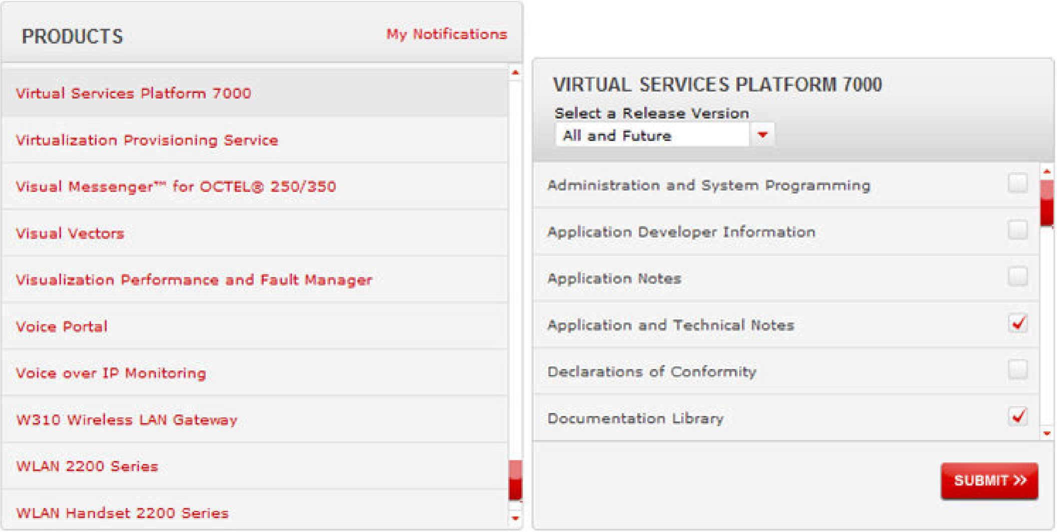
6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.


PRODUCT NOTIFICATIONS

□ Show Details

1 Notices

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



PRODUCTS

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

VIRTUAL SERVICES PLATFORM 7000

Select a Release Version: All and Future

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

11. Click **Submit**.

Support

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

Searching a documentation collection

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

Before you begin

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

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx.
3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
    - Whole Words Only
    - Case-Sensitive
    - Include Bookmarks
    - Include Comments
6. Click **Search**.
   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Chapter 2: New in this release

The following sections detail what is new in *Release Notes for Avaya Virtual Services Platform 7000 Series,* NN47202–400 for Release 10.3

Features

See the following sections for information about feature changes.

ASCII script table

Avaya VSP 7000 Series Release 10.3 provides a table mechanism to load an ASCII configuration file from a USB mass storage device or from a TFTP/SFTP server on a switch or Stack during boot. The table scripts which ASCII configuration file loads on boot. Each entry in the table contains the path to an ASCII configuration file that indicates one of the following ways the file can be downloaded:

- Downloaded from the network using the IP address and filename gotten using BOOTP.
- Downloaded from a TFTP/SFTP server using a specified IP and filename.
- Downloaded from USB using a specified filename and, if in stack, the USB port of a given unit.

The table entries contain a boot priority column. Entries with a lower priority value are loaded first. A non-zero boot priority indicates that the entry can attempt to load at boot time with the specified priority. The table entries also contain the status of the last or current ASCII configuration file download using the file indicated by the entry.

You can display, run, or upload entries from the ASCII script table using the Privileged EXEC mode ACLI command **`script`** with the applicable variables, or using EDM.

You can add or remove entries from the ASCII script table using the Global Configuration mode ACLI command **`script`** with the applicable variables, or using EDM.

For more information, see *Getting Started with Avaya Virtual Services Platform 7000 Series,* NN47202–303.

Content-based forward to next hop

Routers forward data based on the destination address within the packet. However, some circumstances require that packets be forwarded based on criteria other than the destination address. The Content-Based Forward to Next Hop feature forwards packets based on the source IP of the incoming packet. The source address can be an IP address or subnet and a destination TCP/UDP port or range of ports. This feature enables you to isolate packets from certain networks and perform checks on the integrity of the packets or even modify them before forwarding them to the final destination.

Note:

Content-Based Forward to Next Hop works in Layer 3 mode only. Therefore, you must enable routing on the stack/switch to use this feature.

You can define Content-Based Forward to Next Hop policies to specify the source IP and mask to filter and define the next hop to forward the filtered packets. You can also configure Content-Based Forward to Next Hop using the following criteria:

- VLANs – You can apply filter instances to ports on a per VLAN basis. These filter instances are installed only on ports that are members of the VLANs attached to the Content-Based Forward to Next Hop policy.
- Unreachable next hop – When the next hop specified by the policy is unreachable, you can select a **mode** that specifies whether to **drop** the packet or perform **normal routing** based on the destination IP address.

decOtherEther2 protocol VLAN

This feature enables you to create a decOtherEther2 protocol-based VLAN and configure ports as members of this VLAN. The incoming VLAN untagged packets on this port with the Protocol Identifier (PID) field in the decOtherEther2 range of values are switched to the decOtherEther2 VLAN.

You can configure either one of the following, but not both:

- decOtherEther2 protocol-based VLANs
- port-based VLANs with PID in the decOtherEther2 range of values

Note:

The PIDs allowed for decOtherEther2 are (hex): 6000-6003, 6005-6009, and 8038. The decimal values for these are 24576-24579, 24581-24585, and 32824.

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

Diagnostics quick mode flag

The Diagnostics quick mode flag enables you to choose the diagnostic test behavior during boot, either quick mode boot tests, or all the diagnostic tests. The diagnostic quick mode is disabled by default. The impact to boot time is 15–20 seconds when all diagnostic tests run during startup.

In prior releases, all diagnostic tests ran only when the switch was first plugged in. On subsequent boot sequences, quick diagnostics ran, which might cause some errors to miss detection.

You can configure the Diagnostic quick mode flag using ACLI or EDM. In Global Configuration mode, you can use **`diagnostics-quick-mode`** and applicable variables to configure the quick mode diagnostic flag.

For more information, see *Configuring System Monitoring on Avaya Virtual Services Platform 7000 Series,* NN47202–505.

Dynamic routing over SMLT scaling

Avaya VSP 7000 Series Release 10.3 enhances dynamic routing protocol over Switch Cluster support by increasing the Open Shortest Path First (OSFP) over Split Multi-Link Trunking (SMLT) capacity, and adds support for Routing Information Protocol (RIP) over SMLT. A maximum of 64 OSPF and RIP interfaces over SMLT are supported.

Previous releases introduced static routing over SMLT, and dynamic routing protocol over SMLT to distribute routes across the SMLT/SLT network. Dynamic routing over SMLT and Layer 3 traffic can provide seamless recovery if one of the interfaces goes down, reducing the administrative load in a large network.

EDM improved download support

EDM displays the following status messages while downloading software:

- If you are downloading software using the **NoReset** option, EDM displays the following messages:
  - A software download progress percentage to indicate the time taken to download the software to the unit.
  - For software, a message stating that the `Download successfully completed.`

  - For an image or diagnostics, a message stating that the `Download successfully completed. You will need to reboot the switch for changes to take effect. Do you want to reboot now [Yes] [No]`

- If you are downloading software and NOT using the **NoReset** option, EDM displays the download progress percentage, the `Download successfully completed.` message, a message that the switch is being rebooted, and an estimate of the time remaining (5 minutes).

  After rebooting, EDM attempts to reconnect to the switch. If it cannot reconnect immediately, then it shows the estimated reattempt time. For example, the time taken to reconnect can be 30 seconds.

For more information, see *Using ACLI and EDM on Avaya Virtual Services Platform 7000 Series,* NN47202–101.

EDM Stack Forced Mode

Avaya VSP 7000 Series Release 10.3 adds EDM support for Stack Forced Mode. The Stack Forced Mode feature was introduced in a previous release. You can now configure Stack Forced Mode using ACLI or EDM.

Stack Forced Mode allows one or both units to become standalone switches if a stack of two units fails. With Stack Forced Mode, you can manage one of the standalone devices from a failed stack of two with the previous stack IP address.

For more information, see *Getting Started with Avaya Virtual Services Platform 7000 Series,* NN47202–303.

Fabric Connect command changes

Release 10.3 changes ACLI commands for Avaya VENA Fabric Connect to align with the commands used on other Avaya products.

The following table identifies the commands with changed syntax. The original commands still work but do not appear in the ACLI Help text.

Table 1: Command syntax changes

Old command	New command
`l2ping vlan`	**`l2 ping vlan`**
`l2traceroute vlan`	**`l2 traceroute vlan`**
`l2tracetree vlan`	**`l2 tracetree vlan`**

The following table identifies the commands with other changes.

Table 2: Other command changes

Command	Change
`show isis spbm`	The output of the command is modified to display enable or disable instead of true or false for lsdp trap status.
`show isis spbm nick-name`	The output of the command is modified to display the number of entries.
`show isis spbm unicast-fib [b-mac <b-mac>] [vlan <vlan-id>] [summary]`	The output of the command is modified to refer to the local system as cpp in the OUTGOING column.
`min-lsp-gen-interval <min-lsp-interval>`	The command is obsolete.
`show cfm spbm`	The output of the command is modified to appear in a tabular form and include a MAC column.

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

Fabric Connect and Distributed Top-of-Rack interoperability

Avaya VSP 7000 Series Release 10.3 enhances the support of Fabric Connect and DToR interoperability introduced in Release 10.2.1. Fabric Connect can support a Stack-mode DToR of up to eight units, which provides an additional level of resiliency for UNI-attached devices.

Fabric Connect and Switch Cluster interoperability

Fabric Connect refers to the MAC-in-MAC variant of IEEE 802.1aq Shortest Path Bridging (SPB), Intermediate System to Intermediate System (IS-IS), Connectivity Fault Management (CFM), and Avaya enhancements to features and services that leverage SPB technology. Fabric Connect provides a logical Ethernet network infrastructure using a link state protocol to advertise both topology and logical network membership.

Switch Cluster, which is also referred to as Split Multi-Link Trunk (SMLT), is a Layer 2 (L2) feature that allows two aggregation switches to function as one logical unit to provide enhanced load sharing and faster error recovery.

Release 10.3 adds support for Fabric Connect and Switch Cluster interoperability, also known as SPB over SMLT, in the following topologies:

- Triangle-SMLT – This topology consists of one pair of aggregation units and one or two access units.
- Square-SMLT – This topology consists of two pairs of aggregation units that are connected back to back.

The aggregation unit can be a single Switch or a Stack. There is no restriction on the number of units in the SMLT Stack, but for better recovery Avaya recommends a Stack of at least three units. In the Stack, IST and SMLT trunks can be either MLT or DMLT trunks. Avaya also recommends having at least one IST port residing on the base unit for better performance. You can configure SLT ports on any unit within the Stack.

Note:

SMLT is supported on UNI ports only. SMLT on NNI ports are not supported.

FastEthernet replaced with Ethernet

Avaya VSP 7000 Series Release 10.3 replaces **`FastEthernet`** with **`Ethernet`** as the interface mode ACLI variable.

For configuration compliance, **FastEthernet** is hidden, but remains functional to support configuration scripts from previous releases.

Note:

ASCII configurations saved from Release 10.3 or later cannot be used to configure a unit running a previous software release that does not support the **`Ethernet`** command.

Feature licensing

Beginning with Release 10.3, all features are supported with the VSP 7000 Series Base license, and no additional licensing is required. All references to licensing for specific features are removed from this guide.

Fibre Channel over Ethernet Redirect

Fibre Channel over Ethernet (FCoE) enables the consolidation of both storage area network (SAN) and Ethernet traffic onto one 10 Gigabit Ethernet (10GE) common network. This feature supports connectivity for FCoE devices, or e-nodes, to a standard Ethernet switching platform without the need for dedicated FCoE switches. It also eliminates the need for a local FCoE gateway, which is normally required for all e-node devices in the same physical location.

FCoE Redirect uses an external FCoE Network Controller (FNC) to virtualize the FCoE control plane and configure the switch to facilitate FCoE forwarding. The FCoE Redirect and FNC are key components in the Avaya Software-Defined SAN solution. This solution manages a physical network as a virtualized logical network, by separating the data and control planes of the network. This approach allows the dynamic creation of networks that support virtualization across the entire network. Also, a Software-Defined Storage Area Network (SDSAN) can be managed as a single entity, greatly simplifying the deployment and management of the network.

FCoE Redirect function requires an external FNC. You can purchase a license for the FNC software. Each license supports 32 FCoE devices.

You can configure FCoE Redirect on Virtual Services Platform 7000 Series using ACLI or EDM. You must install and configure the FNC software separately.

This feature is a Controlled Introduction feature for Release 10.3. For more information on how to install and configure Avaya Software-Defined SAN, see *Deploying Avaya Software-Defined SAN Using Avaya VSP 7000 Series*, NN47202–306.

Flash History

The Flash History feature provides counters that show flash activity. This feature addresses the problem where excessive writes to flash cause a failure. The **`show flash history`** command provides information on how often the flash device is accessed. You can review this information during debugging or development activities to identify what processes are writing excessively to flash.

You can use this command to view the flash writes and erase history on a standalone unit or stack. The Flash History does not record programming from the diagnostics or bootloader. Flash History information is stored in the Serial (PC) Electrically Erasable Programmable Read Only Memory (SEEPROM). The data does not corrupt during an upgrade or downgrade. Flash History is enabled by default and does not require any configuration.

For more information, see *Configuring System Monitoring on Avaya Virtual Services Platform 7000 Series,* NN47202–505.

IGMP over SMLT

Avaya VSP 7000 Series Release 10.3 introduces the ability to support Internet Group Management Protocol (IGMP) over Split Multi-Link Trunking (SMLT) network topologies. This feature ensures that multicast traffic is not interrupted even if one of the units in a Switch Cluster fails. It also ensures that IGMP group membership and dynamic mrouter ports are in sync on both SMLT peers.

To support IGMP over SMLT, the following basic operations are performed:

- The groups on one SMLT aggregation switch populate to the other SMLT aggregation switch over the IST to have a redundant path (Wiring Closet Switch). IGMP IST report messages forward only to query ports and not IST links. If the report is received over SMLT, then SMLT links configure as the member ports for that group.

  Note:

  If the IST group report message does not have SMLT ID information, then IST links configure as the member ports for the group.

- IGMP queries received on an aggregation switch are flooded to all links (except the IST links) in the VLAN. IGMP queries reaching one aggregation switch populate to the other aggregation switch using IST query messages. The aggregation switch uses the SMLT ID in the query message to configure the SMLT links as the querier ports. If an SMLT link goes down, the querier port moves to the IST link to ensure that IGMP reports always forward to the IGMP querier or PIM router.

  Note:

  If the IGMP query is received on a link or MLT (not SMLT), the SMLT ID is set to zero in the message. The aggregation switch that receives the IST query message uses the SMLT ID in the query message to configure the SMLT links as the querier ports. If the IST query message does not have an SMLT ID (SMLT ID = 0), then the IST link configures as the querier port.

- IGMP leave messages received on an aggregation switch are treated in the same way as IGMP reports. Leave messages are sent to the other aggregation switch over IST links in IST leave messages. The aggregation switch that receives the IST leave message removes the group membership for that member. If a switch has no more receivers for a group (receivers on SMLT links are exempted), switch sends an IST IGMP prune option. The switch that receives the IST IGMP leave with prune, removes the group membership of the IST link (if it exists).
- IST messages are defined for different IGMP packet types. The different message types supported are:
  - `IST IGMP Query` - contains the source IP address (querier IP address), VLAN, Group Address (in the case of group specific query), maximum response time and the SMLT ID (in the case IGMP queries are received on an SMLT).
  - `IST IGMP Group Query`
  - `IST IGMP Group Report` - contains a source IP address, group address, VLAN, and SMLT.
  - `IST IGMP Group Leave`
- There are two types of SMLT messages that are processed by IGMP:
  - `IGMP_PEER_SMLT_DOWN`: The SMLT peer that receives this message sends IST IGMP group reports to the other peer for all members of that specific SMLT. The

SMLT id is set to 0, so all reports are learned on the other peer's IST port (also applicable to the querier if it is located on a port member).

- `IGMP_PEER_SMLT_UP`: Same as IGMP_PEER_SMLT_DOWN, however the SMLT id is set to the proper value.

- If an SMLT peer receives an SMLT IGMP message and the SMLT id specified in that message is down, the IST port is programmed instead. The IST must be up and the specified SMLT must be configured.

Note:

ACLI or EDM commands are not required for this feature interaction.

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

ip.cfg console status messages

You can load the `ip.cfg` file from the USB memory device as to pre-stage the IP address and other parameters for the operation of a switch. You can specify one or more of the optional parameters in the `ip.cfg` file.

In this release, whenever the switch executes an instruction from the `ip.cfg` file, a status message displays on the console and a message is added to the system log. In previous releases, there were no status messages to indicate any progress.

Note:

If more than one USB device containing valid `ip.cfg` files are inserted into a Stack, only the Base Unit shows the console status messages and displays the current applied settings.

To ensure that the Base Unit prints messages, do not access Non-Base Units with USB `ip.cfg` files for at least 15-30 seconds after the banner is printed.

You should verify that the commands from the `ip.cfg` file (such as IP address, network mask, VLAN and others) are correct in the status messages. You can use the ACLI command **`show usb-files ascii IP.CFG <unit#>`** to verify the configuration.

For more information, see *Getting Started with Avaya Virtual Services Platform 7000 Series,* NN47202–303.

IP netstat

The **`show ip netstat`** command displays information about active IPv4 sockets.

The following example shows the results of the **show ip netstat** command:

```
7024XLS>show ip netstat
Proto Recv-Q Send-Q  Local Address         Foreign Address       State
----- ------ ------  --------------------- --------------------- -----------
TCP        0      0  0.0.0.0.23            0.0.0.0.0             LISTEN
TCP        0      0  0.0.0.0.80            0.0.0.0.0             LISTEN
TCP        0      3  172.10.100.150.23     209.171.150.60.1553   ESTABLISHED
UDP        0      0  0.0.0.0.161           0.0.0.0.0
UDP        0      0  0.0.0.0.0             0.0.0.0.0
UDP        0      0  0.0.0.0.0             0.0.0.0.0
UDP        0      0  172.10.100.150.3491   0.0.0.0.0
----------------------------------------------------------------------------
Proto Port  Service
----- ----- -------
TCP   23    TELNET
TCP   80    HTTP
UDP   161   SNMP
UDP   3491  RADIUS
```

IPv6 automatic address assignment

Avaya VSP 7000 Series Release 10.3 supports IPv6 automatic address assignment. When IPv6 routing is enabled for an interface, or when an IPv6 address is configured on an interface, the system automatically creates an IPv6 local route entry in the IPv6 routing table. The IPv6 automatic address assignment can function with the following limitations:

- IPv6 forwarding must be enabled.
- Maximum of one IPv6 address on each interface.
- Maximum of 256 neighbor discovery prefixes, and you can assign more than one prefix to each VLAN.

Each IPv6 neighbor discovery prefix with local routes is added automatically to the IPv6 routing table.

You can configure IPv6 neighbor discovery prefixes using ACLI or EDM.

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

IPv6 DHCP Relay

Avaya VSP 7000 Series Release 10.3 supports IPv6 DHCP Relay. IPv6 DHCP Relay allows the routing switch to act as an IPv6 DHCP (or DHCPv6) relay agent, as described in*RFC 3315*, Dynamic Host Configuration Protocol for IPv6 (DHCPv6).

A DHCPv6 relay agent is used to relay messages between a DHCPv6 client and a DHCPv6 server connected to different VLANs. IPv6 DHCP Relay function requires IPv6 static routes.

DHCP for IPv6 enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. DHCP supports automatic allocation of reusable network addresses and of additional configuration parameters.

You can configure IPv6 DHCP Relay forward paths, and view or clear IPv6 DHCP Relay counters using ACLI or EDM. A maximum of 256 forward paths are supported.

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

IPv6 in IPv4 tunnels

Avaya VSP 7000 Series Release 10.3 supports IPv6 in IPv4 tunnels. This feature enables isolated IPv6 sites to communicate with other IPv6 sites by encapsulating IPv6 packets in IPv4 packets through an IPv4 network. IPv6 in IPv4 tunnels supports the 6to4 specification in RFC 4213.

You must manually configure the IPv6 address of the tunnel interface and the IPv4 addresses of the endpoints. A maximum of four tunnel end points is supported. You can configure and view IPv6 in IPv4 tunnels using ACLI or EDM.

You can use tunnels on any Layer 3 VLAN but only for management traffic.

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

IPv6 Out-of-band management

Avaya VSP 7000 Series Release 10.3 enhances Out-of-band management with IPv6 support. IPv6 is supported for switch or stack management using the dedicated out-of-band management port. Out-of-band management supports Telnet, Secure Shell (SSH) protocol, Simple Network Management Protocol (SNMP), HTTP, or HTTPS, without requiring an in-band management VLAN.

To configure out-of-band management, you can assign an IPv4 or IPv6 address to the RJ-45 Ethernet management port for a switch or stack. You can configure a specific out-of-band management default gateway, which takes precedence over the in-band default gateway. If you do not configure an out-of-band management default gateway, the in-band default gateway is used for out-of-band switch or stack management.

> **Note:**
>
> The out-of-band switch or stack management IP address must be different than the in-band IP address and belong to a different subnet.

You can use the out-of-band management port to perform tasks such as downloading software images and, when the SNMP server is enabled, access the Enterprise Device Manager (EDM) interface for a switch or stack. To access EDM, you type the out-of-band management address in the address bar of an Internet browser.

The out-of-band management port supports full auto negotiation, which enables management stations to connect at any of the supported speeds or duplexes.

For more information, considerations, and limitations, see *Getting Started with Avaya Virtual Services Platform 7000 Series,* NN47202–303.

IPv6 static routes

Avaya VSP 7000 Series Release 10.3 provides support for configuring multiple IPv6 static routes and IPv6 routes for each VLAN.

Static routes provide a method for establishing route reachability. This function provides routing information from the forwarding database to the forwarding plane. Only enabled static routes are submitted to the Route Table Manager (RTM), which determines the best route based on reachability, route preference, and cost. The RTM communicates all updates to best routes to the forwarding plane.

Supported features include the following:

- Multiple configurable IPv6 interfaces associated with VLANs
- Multiple IPv6 global addresses (automatically inserted into the routing table) for each IPv6 interface
- Multiple configurable static route entries in the IPv6 routing table
- Router functionality based on the routing table constructed using the two preceding methods listed
- User-configured prefix lists that are advertised to hosts for stateless autoconfiguration

A maximum of 512 IPv6 static routes are supported. IPv6 static route function requires global IPv6 routing and IPv6 admin status enabled.

You can configure IPv6 static routes using ACLI or EDM.

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

IPv6 VLAN support

Avaya VSP 7000 Series Release 10.3 supports the configuration of IPv6 VLAN interfaces, IPv6 addresses, and IPv6 forwarding.

- A maximum of 256 IPv6 VLAN interfaces
- A maximum of 256 IPv6 global addresses, one for each IPv6 VLAN interface (automatically inserted into the routing table).

You can configure IPv6 VLANs using ACLI or EDM.

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

Jumbo frames

Avaya VSP 7000 Series Release 10.3 allows you to customize the jumbo frame size, and jumbo frames are enabled by default. A jumbo frame is an Ethernet frame that is larger than 1518 bytes. Following are benefits of jumbo frames:

- Each frame carries a larger payload as the header sizes remain the same.
- There are fewer interrupts on the server due to less frames and a smaller CPU load.
- Larger frames provide better buffer utilization and forwarding performance in switches.

The default jumbo frame size is 9216 bytes. You can configure the jumbo frame size between 1519 and 9216 bytes. When jumbo frames are disabled, the maximum frame size is 1518.

You can configure jumbo frames using ACLI or EDM.

For more information, see *Getting Started with Avaya Virtual Services Platform 7000 Series,* NN47202–303.

Link State Tracking

Link State Tracking (LST) binds the link state of multiple interfaces. If a specified interface or its Virtual Link Aggregation Protocol (VLACP) state goes down, then all other interfaces in that group enter a temporary down state. For example, LST can provide application redundancy in the network with two separate units or Stacks when utilized with server Network Interface Card (NIC) teaming. If interface 1 goes down on either switch, the server continues to send traffic through interface 2 and the traffic is dropped. If interfaces 1 and 2 are coupled in a link-state group (as upstream and downstream ports respectively), when interface 1 is unavailable, interface 2 is disabled prompting the server to choose the other path as target.

LST identifies the upstream and downstream interfaces. Interfaces connected to servers are downstream interfaces, and interfaces connected to distribution switches and network devices are upstream interfaces. In a link state group, these interfaces bundle together and the downstream interfaces are bound to the upstream interfaces.

When you enable link-state tracking on the switch, the link state of the downstream ports is bound to the link state of one or more of the upstream ports. Upstream or downstream interfaces can include switch ports or trunk members (MLT/DMLT/LAG). After you associate a set of downstream ports to a set of upstream ports, if all of the upstream ports for that group become unavailable, then link-state tracking automatically changes the associated downstream ports into a temporary disabled state. In scenarios where a server is dual homed to the switch, the server primary interface can fail over to the secondary interface.

Each downstream interface can be associated with a single group consisting of multiple upstream interfaces, referred to as a link-state group. If all of the upstream interfaces in a link-state group are in a link-down state, the associated downstream interfaces are forced into a link-down state. If any one of the upstream interfaces in the link-state group is in a link-up state, the associated downstream interfaces are allowed to change to, or remain in a link-up state.

You can configure a maximum of two link-state groups.

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

MDA hot swap

Avaya VSP 7000 Series Release 10.3 supports the hot swapping of the Media Dependent Adapter (MDA) module. This means that you can insert or remove an MDA while the unit is operating. You can also swap one MDA type for another without the need to reset the switch or issue a command after insertion. For example, you can Hot Remove a 7008XLS MDA and then Hot Insert a 7008XT MDA. Previous releases supported MDA warm swap only.

The **`mda`** command controls the administrative status of the MDA card: enabled or disabled. By default, MDA ports are enabled.

Hot Removal

- Hot removal of an MDA is allowed, and does not cause a reboot or unexpected operations within the switch or stack.
- Before you hot remove an MDA, Avaya recommends you use the **`no mda enable`** command to stop forwarding traffic to the MDA ports. This action reduces the occurrence of traffic loss when the MDA is removed. Otherwise, if the MDA is hot removed, then any traffic queued to the MDA ports is lost.

Hot Insertion

- Hot insertion of an MDA is allowed, and does not interrupt traffic within the switch or stack.
- After hot inserting an MDA, the switch can access and use the MDA without needing to be reset. If the MDA status is enabled, no commands are required.

For more information, see *Getting Started with Avaya Virtual Services Platform 7000 Series,* NN47202–303.

Network Time Protocol

Avaya VSP 7000 Series Release 10.3 adds support for Network Time Protocol (NTP).

Units can now support either Simple Network Time Protocol (SNTP) or NTP for time synchronization. This support extends to both primary and secondary servers, using IPv4 or IPv6.

NTP can provide a more reliable and secure time synchronization as compared to SNTP. NTP supports the option to authenticate NTP connections to the server, thereby ensuring a secure means of information exchange from known or trusted servers. You can configure NTP with up to 10 IPv4 servers.

You can configure NTP using ACLI or EDM.

For more information, see *Getting Started with Avaya Virtual Services Platform 7000 Series,* NN47202–303.

Non-unicast MLT hashing

The non-unicast MLT hashing feature enables multicast and broadcast layer 2 traffic to be distributed on ***all*** trunk members. In previous releases, multicast and broadcast traffic was always sent on the first active link in the MLT trunk group (Link 1). This feature improves load balancing by ensuring better distribution of non-unicast traffic on MLT ports.

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

QoS agent buffer

Release 10.3 adds the spb-scaled parameter to the **`qos agent buffer`** command.

Use this parameter to select an amount of resource sharing specifically designed for large SPBM configurations. When you enable SPBM, this mode is automatically selected; when you disable SPBM, the configuration reverts to the default of large.

Note:

If you upgrade from Release 10.2.1 and SPBM is enabled, you must manually run the **`qos agent buffer spb-scaled`** command.

For more information about the `qos agent buffer` command, see *Configuring Quality of Service on Avaya Virtual Services Platform 7000 Series,* NN47202–504.

RO user access to Telnet and SSH

Avaya VSP 7000 Series Release 10.3 supports read-only (RO) user permission to connect from the switch or Stack to another device using Telnet and Secure Shell (SSH) commands. In previous software releases, the Telnet and SSH commands required read-write (RW) user permission.

A secure agent image supports the capability to establish a SSH connection or Telnet session to another SSH or Telnet server device in the network using ACLI. A non-secure agent image supports Telnet sessions only.

In RO mode, you can establish a SSH connection to another SSH server using DSA public key authentication, RSA public key authentication, or password authentication. In RO mode, you can establish a Telnet connection to another Telnet server using password authentication.

RSPAN

Remote Switch Port Analyzer (RSPAN), also known as Remote Port Mirroring, enhances port mirroring by enabling mirrored traffic to be sent to one or more switches or stacks in the network using an RSPAN VLAN to forward the mirrored traffic. All participating switches must support the RSPAN feature.

RSPAN enables you to monitor traffic by making a copy of each incoming and outgoing packet to and from a port according to a set of rules. RSPAN consists of at least one port mirroring source session, an RSPAN VLAN, and at least one RSPAN destination session. You must configure these items on different devices on the network.

The traffic for each RSPAN session is transmitted through the RSPAN VLAN that you configure. The RSPAN traffic from the source ports or VLANs is copied into the RSPAN VLAN and is forwarded over trunk ports carrying the RSPAN VLAN to a RSPAN destination session. Each RSPAN source switch must have either ports or VLANs as RSPAN sources. The final destination must be a physical port.

RSPAN dependencies, limitations, and restrictions are the following:

- All units must support a RSPAN VLAN and compatible RSPAN functions.
- A maximum of four RSPAN destination sessions, each session is one port, therefore a maximum of four destination ports on each unit.
- A maximum of four RSPAN VLANs on each unit.
- A RSPAN VLAN or RSPAN port cannot be used in another RSPAN session.

- A RSPAN VLAN cannot be configured as a management VLAN.
- A RSPAN session must be deleted before you can modify a RSPAN VLAN, or RSPAN destination port.
- All RSPAN VLAN traffic is flooded, no MAC address learning occurs on the RSPAN VLAN, and RSPAN traffic can be terminated on supporting units.
- Any port in a Stack can be specified as for RSPAN, with the following exceptions:
    - A port with 802.1X enabled cannot be a RSPAN destination port.
    - A port that is a member of a MLT, DMLT, or LAG cannot be a RSPAN destination port, but it can be a RSPAN source port.
    - A port that is a RSPAN source or mirrored port cannot be a RSPAN destination port.
    - A port cannot be configured with the allow-traffic option in an RSPAN VLAN.
    - A port requires filters (and system resources) to be a RSPAN source in the following port mirroring modes:
        - MAC based mode: Asrc, Adst, AsrcBdst, AsrcBdstOrBsrcAdst, AscrOrAdst
        - Port based mode: XrxYtx, XrxYtxOrYrxXtx
- Layer 3 routed traffic displays incorrect port mirroring source and destination MAC information, since mirroring is performed as the last operation.
- A RSPAN session does not mirror CPU generated traffic. Mirrored BPDUs might mix with actual BPDUs and cause STP loops and topology issues.

Note:

Due to hardware limitations, RSPAN is not compatible with VSP 9000 or ERS 8800.

ERS 4500 cannot function as an RSPAN intermediate switch.

You can configure RSPAN using ACLI or EDM. The ACLI command variables for `vlan` and `port-mirroring` are modified to allow for RSPAN configuration.

For more information, see *Configuring System Monitoring on Avaya Virtual Services Platform 7000 Series,* NN47202–505.

run spb script

Avaya VSP 7000 Series Release 10.3 supports an ACLI script to quickly enable Avaya VENA Fabric Connect on a switch or stack.

You can use the command `run spb` to quickly set up the following SPB and IS-IS configuration on a unit:

- Sets the SPB Ethertype.
- Creates an SPB instance.
- Creates an SPB primary and secondary B-VLAN.
- Adds an SPB nickname.
- Creates a manual area.
- Enables IS-IS on one of the switch interfaces.
- Sets the IS-IS system name.
- Sets the IS-IS system ID.

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

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

SFP+ devices

In addition to the SFP+ devices currently supported, Release 10.3 adds support for SFP+ 10GBASE-ZR/ZW and CWDM devices for increased connectivity options and reach.

The following table describes the new 10GBASE-ZR/ZW SFP+ device:

Model number	Product number	Description
10GBASE-ZR/ZW	AA1403016-E6	1-port 10GBase-ZR/ZW SFP+

The CWDM SFP+ devices are all 1-port Ethernet transceivers that are Lucent connector (LC) type. They are also Diagnostic Monitoring Interfaces (DDI) that support Digital Diagnostic Monitoring (DDM). DDM allows the VSP 7000 to monitor SFP laser operating characteristics.

The following table describes the new CWDM SFP+ devices:

Model number	Product number	Description
CWDM SFP+	AA1403153-E6	1470 nm. The range is 40 km.
CWDM SFP+	AA1403154-E6	1490 nm. The range is 40 km.
CWDM SFP+	AA1403155-E6	1510 nm. The range is 40 km.
CWDM SFP+	AA1403156-E6	1530 nm. The range is 40 km.
CWDM SFP+	AA1403157-E6	1550 nm. The range is 40 km.
CWDM SFP+	AA1403158-E6	1570 nm. The range is 40 km.

Model number	Product number	Description
CWDM SFP+	AA1403159-E6	1590 nm. The range is 40 km.
CWDM SFP+	AA1403160-E6	1610 nm. The range is 40 km.
CWDM SFP+	AA1403161-E6	1470 nm. The range is 70 km.
CWDM SFP+	AA1403162-E6	1490 nm. The range is 70 km.
CWDM SFP+	AA1403163-E6	1510 nm. The range is 70 km.
CWDM SFP+	AA1403164-E6	1530 nm. The range is 70 km.
CWDM SFP+	AA1403165-E6	1550 nm. The range is 70 km.
CWDM SFP+	AA1403166-E6	1570 nm. The range is 70 km.
CWDM SFP+	AA1403167-E6	1590 nm. The range is 70 km.
CWDM SFP+	AA1403168-E6	1610 nm. The range is 70 km.

For more information on these and previously supported SFP+ devices, see *Installing Transceivers and Optical Components on Avaya Virtual Services Platform 7000 Series,* NN47202–302.

SFP DDI information

The Digital Diagnostic Interface (DDI) feature collects data and monitors alarms and warnings on all the supported SFP, SFP+, and GBIC transceivers. The following lists the information that DDI collects:

- SFP vendor information (including type, wavelength, vendor name, vendor revision/serial, hardware options, CLEI code, and Product Code)
- DDI support information
- DDI alarm and warning threshold values
- temperature
- supply voltage
- transmit bias current
- TX/RX optical power
- transmit power
- receive power measurement
- transceiver calibration

This functionality is supported from the moment the switch finishes its initialization.

For more information, see *Configuring System Monitoring on Avaya Virtual Services Platform 7000 Series,* NN47202–505.

SFP log and trap entries

Avaya VSP 7000 Series Release 10.3 adds log messages and SNMP trap entries when SFP devices are inserted or removed from a unit.

SLA Mon Phase 2

Avaya VSP 7000 Series Release 10.3 enhances the SLA Mon™ Technology agent as part of the Avaya SLA Mon solution. SLA Mon uses a server and agent relationship to perform end-to-end network Quality of Service (QoS) validation, and acts as a distributed monitoring device. You can use the test results to target under-performing areas of the network for deeper analysis.

In SLA Mon Phase 1, the SLA Mon agent only supported clear text communication between the Avaya Diagnostic Server and the SLA Mon agent. It did not support encrypted agent-server communication.

With Release 10.3, SLA Mon Phase 2 supports the following modes of communication:

- Certificate-based authentication (TLS-based)
- Encrypted agent-server communication
- Clear text communication

The VSP 7000 agent image determines which communication mode to use. Secure images use either the authentication or the encryption mode while non-secure images use clear text. SLA Mon Phase 2 agents also support the integration of SLA Mon tests into the CLI for administrator use in the absence ofAvaya Diagnostic Server with SLA Mon™ support.

You can configure SLA Mon using ACLI or EDM.

For more information, see *Configuring System Monitoring on Avaya Virtual Services Platform 7000 Series,* NN47202–505.

SLPP Guard

Avaya VSP 7000 Series Release 10.2 supports Simple Loop Prevention Protocol (SLPP) Guard. You can use SLPP Guard in combination with Avaya's Split Multi-Link Trunking (SMLT) to provide additional loop protection to protect wiring closets from erroneous connections. SMLT implementations provide an SLPP packet, which helps prevent loops from occurring when switch clustering is implemented. When you enable SLPP Guard, this loop prevention mechanism extends into and across multiple wiring closets. If the edge switch configured for SLPP Guard receives an SLPP packet on a port, the feature administratively disables the port and generates log messages and SNMP traps.

SLPP is necessary for loop protection as STP/MSTP/RSTP must be disabled on links to SMLT switches.

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

SMLT over LACP scaling

Split Multi-Link Trunk (SMLT) over Link Aggregation Control Protocol (LACP) can improve trunk resilience and handling in a failover situation. Avaya VSP 7000 Series Release 10.3 increases the scaling to support a maximum:

- 20 SMLT over LACP links
- 100 SLT over LACP links

SMLT is also referred to as Switch Cluster.

SSH RSA authentication

SSH RSA authentication provides increased security for Secure Shell (SSH) login. With this feature, the switch supports RSA public-private key encryption that uses a digital certificate for SSH login.

SSH RSA authentication is supported when you select the RSA certificate option for a Secure Shell connection from a client PC to the switch.

For more information, see *Configuring Security on Avaya Virtual Services Platform 7000 Series,* NN47202–501.

Stack protection from duplicate base units

> **Important:**
>
> If you power cycle a stack and there is more than one unit with the base unit switch enabled, the stack will not form after boot even if the stack was operational before the reset.

This feature protects the operational integrity of the stack even after adding a new or replacement unit with the base unit switch enabled. The following scenarios describe how this feature protects the stack:

- If a unit with the base unit switch enabled is added to an operational stack, it is ignored. The stack continues operating as it was before, and the added unit runs in standalone mode. A log message on the new unit and on the base unit of the stack informs the user of this action.

Note:

Avaya recommends that you disable the base unit switch on the new unit.

- If an operational stack is running in temporary base mode, any new unit is added regardless of the base unit switch position. (The only limitation is that the stack cannot exceed eight units.) Again, if you power cycle a stack and there is more than one unit with the base unit switch enabled, the stack will not form after boot.

Static LACP key to trunk ID binding

Avaya VSP 7000 Series Release 10.3 allows you to control the trunk group assignment through a static association between the Link Aggregation Control Protocol (LACP) key of the LACP ports and the trunk group ID. The maximum number of key-to-trunk ID associations is bound to the maximum number of MLT trunks that can be configured on the device (64 trunks). In previous releases, the trunk group assignment was dynamic.

LACP is a standard that groups multiple physical Ethernet links together to act as a single link. The group is called a LACP aggregation group (LAG). This grouping provides redundancy for the physical connection between the devices at the ends of the physical links.

LACP assigns a key that binds the group together and identifies the LAG. The LAG then becomes part of a trunk group to become functional and forward traffic.

This Static LACP key to trunk ID binding feature gives you more control over the association between LACP ports and trunk groups than dynamic binding. For backwards compatibility both methods are available. However, when the static method is set, it overrides the dynamic method.

Note:

Avaya recommends you to use the Static LACP key to trunk ID binding because it can prevent undesired configurations. For example, if you configure two LACP trunks, the MLT IDs are assigned to each trunk in the order of their creation. If the device is rebooted, the order that each LAG receives a trunk might invert and the LACP aggregator might receive a different trunk than what was intended. The Static LACP key to trunk ID binding feature association between LAGs and MLT IDs can prevent this problem.

Important:

With Static LACP key to trunk ID binding, you must keep track of the used trunk IDs. Binding multiple keys to different trunks may easily lead to the use of all available MLT IDs. If all MLT IDs are used, you cannot configure a new LACP trunk, even if all the other required conditions for trunk formation are accomplished.

You can use the **`show lacp key`** command to display the LACP key bindings in use.

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

Transparent UNI

Transparent UNI (T-UNI) assigns a port or MLT to an I-SID. This feature configures a transparent port where all traffic is MAC switched on an internal virtual port (I-SID). Multiple ports on the same unit and on other Backbone Edge Bridges (BEBs) are switched on a common I-SID. A port or MLT you assign to an I-SID as a Transparent UNI is referred to as a T-UNI port.

The T-UNI ports are fully transparent since tagged and untagged traffic is switched within the assigned I-SID, as well as any control protocol. T-UNI ports are not members of any VLAN, or any STG. T-UNI ports are always in a forwarding state.

MAC learning is against the I-SID and the port or MLT instead of the C-VLAN. When a packet ingresses on a port or MLT that is associated with a T-UNI I-SID, the MAC lookup performs based on I-SID.

This feature is called transparent because the MAC learning is against the I-SID and packets ingressing with any C-VLAN process in exactly the same way. Also, because the service classification of the packets received on a T-UNI port is independent of any VLAN-ID values that might be present on the packet. All data packets received on the port are classified into the same service. No VLAN tag modifications are performed on the data packets as they enter and exit the T-UNI service.

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

USB log and trap entries

Avaya VSP 7000 Series Release 10.3 adds log messages and SNMP trap entries when USB devices are inserted or removed from a unit.

UTC timestamp

The UTC timestamp feature displays a timestamp immediately after you enter a **`show`** command and before the output displays. This enables you to monitor the exact time for specific configurations.

You can enable or disable the UTC timestamp using the ACLI global configuration command **`cli timestamp`** with appropriate variables. The UTC timestamp is disabled by default.

Other changes

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

Documentation title changes

The documentation titles are revised for Avaya VSP 7000 Series Release 10.3. For a full list of associated product documentation, see *Documentation Roadmap Reference for Avaya Virtual Services Platform 7000 Series,* NN47202–103.

Filter resource consumption

Release 10.3 adds Filter resource consumption on page 71 to this document.

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.

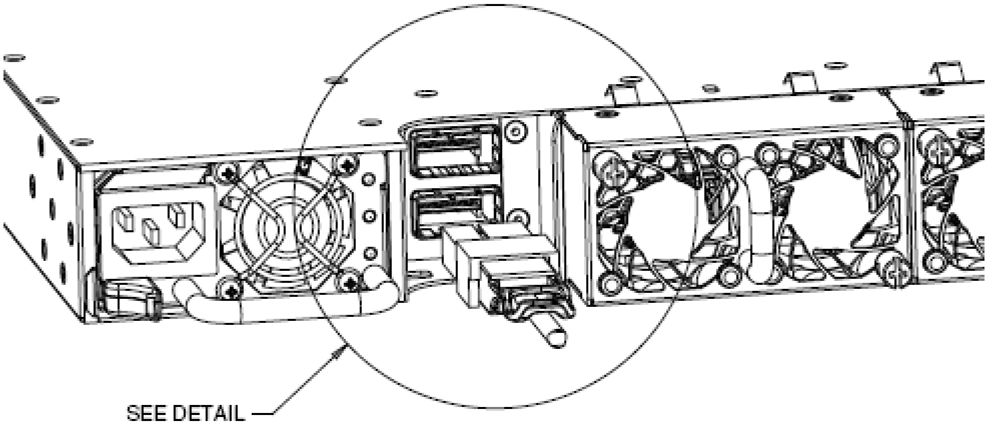
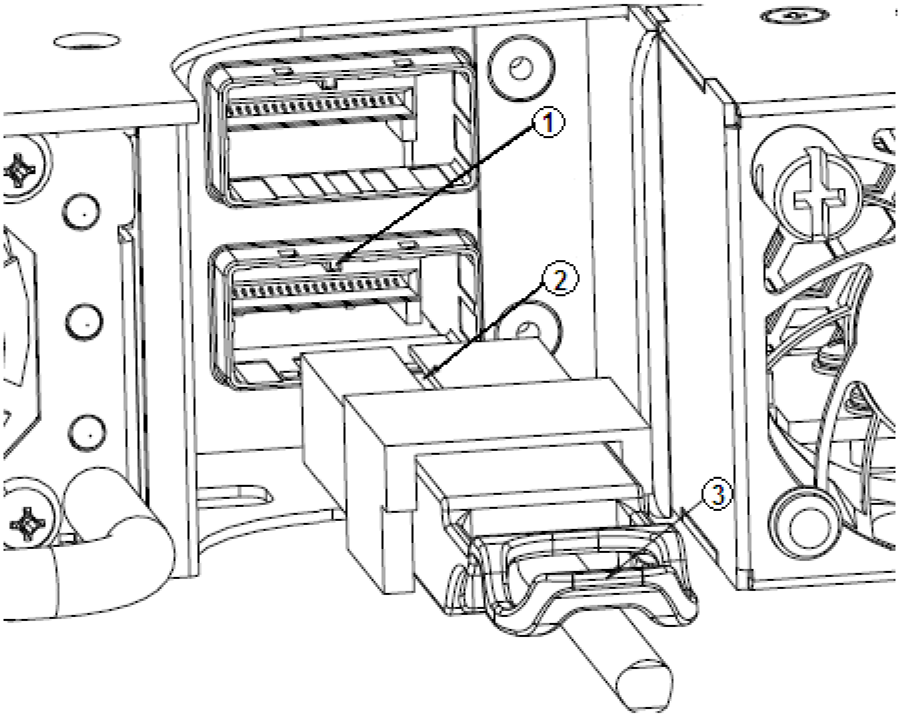


Figure 1: Installing Fabric Interconnect cables



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

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 10.3 software files. File sizes are approximate.

Module or file type	Description	File name	File size (bytes)
Standard runtime image for Release 10.3.	Agent software image for the Avaya Virtual Services Platform 7000 Series	7000_1030010.img— non-secure image 7000_1030011s.img— secure image	11,282,228 11,542,020
Diagnostics software for Release 10.3.	Diagnostics software for the Avaya Virtual Services Platform 7000 Series	7000_10302_diags.bin — diagnostics	3,941,792
MIB definition files for Release 10.3.	MIB definition files	Virtual_Services_Platform_70xx_MIBs_10.3.0.zip	1,284,179
EDM Help files for Release 10.3.	EDM help files	vsp7000v1030_HELP_EDM.zip	4,832,807

Software and hardware capabilities

The following table lists supported software and hardware scaling capabilities for the Avaya Virtual Services Platform 7000 Series Software Release 10.3

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

Feature	Maximum number supported
Layer 2	
Avaya Spanning Tree Groups	8
DHCP Snooping table entries	1,024
MAC addresses	131,071 (32,767 with SMLT)
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	
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

Feature	Maximum number supported
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
VRRP instances	255 IDs (64 active)
Management Routes	4
UDP Forwarding Entries	128
DHCP Relay Entries	256
DHCP Relay Forward Paths	512
Multicast	
IGMP Allow-flood multicast addresses	4096 (The maximum number of allow-flood multicast entries is the aggregate of the number of devices in each VLAN receiving multicast streams.)
IGMP Allow-flood multicast addresses per VLAN	128
IGMP multicast groups	1024
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

Feature	Maximum number supported
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
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

Feature	Maximum number supported
	• 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
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
VENA Fabric Connect (SPB)	
Fabric Connect: operational mode	Standalone or stack

Feature	Maximum number supported
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	11,000 (tested)
Fabric Connect: Switched UNIs	4096
Fabric Connect: nodes per region	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	
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 3.6.x

- Mozilla Firefox 12.x
- Mozilla Firefox 14.x

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..

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

Variable	Value
	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.
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.

Variable	Value
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. • 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.

Variable	Value
	• 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 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 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)

Chapter 4: Resolved issues

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

Resolved issues for Release 10.3

The following table lists the issues resolved in Release 10.3

Reference number	Description
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.
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).

Reference number	Description
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. 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.

Reference number	Description
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 Software Release 10.3. Where available and appropriate, workarounds are provided.

Reference number	Description
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. **Workaround**: You must upgrade from Release 10.0 to 10.1, and then to 10.2. If you accidently upgrade the agent code directly from 10.0 to 10.2 or later, the primary agent image erases and the switch will attempt to boot from the secondary image. You can then perform an upgrade from 10.0 to 10.1, and then to 10.2.
wi01082016	❗ **Important:** **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. **Workaround**: Avaya recommends upgrading all VSP 7000 Series units to the latest software release to ensure Rear-port mode compatibility between units.
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.

Reference number	Description
	Workaround: You must manually configure the unit to the appropriate mode before you retrieve the binary configuration.
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. **Workaround**: The supported browsers for managing a VSP 7000 switch are IE or Firefox. It is recommended to use one of the supported browsers.
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. **Workaround**: Check the FAN status LEDs on the units.
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. **Workaround**: You must configure MLT BPDU send or receive mode using ACLI.
wi00930939	**Netmask**: Modifying the netmask without an IP address might result in connectivity loss. **Workaround**: When modifying the netmask use an IP address in the command: `ip add A.B.C.D mask A.B.C.D`.
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.
wi00971757	**Lossless Mode**: When the switch is operating in Lossless mode and flowcontrol is disabled on a port, the dropped on

Reference number	Description
	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.
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. **Workaround:** Working as designed. If you require ISIS to be enabled only on some rear-ports (Fabric Interconnect), you can group specific ports into LAGs according to LACP keys, and apply ISIS to the desired LAG.
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. **Workaround:** Working as designed. If you require ISIS to be enabled only on some rear-ports (Fabric Interconnect), you can group specific ports into LAGs according to LACP keys, and apply ISIS to the desired LAG.
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. **Workaround:** Working as designed. If you require different parameters on specific rear-ports (Fabric Interconnect), you can group specific ports into LAGs according to LACP keys..
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.
wi01040581	**Rear-port mode, full default**: If you fully default a switch operating in rear-port mode, the rear-port mode is disabled.

Reference number	Description
	Upon reboot, the fully defaulted unit attempts to join a FI stack, causing other connected units operating in rear-port mode to crash. **Workaround**: Before performing a full default on a unit operating in rear-port mode, disconnect the FI cables on the unit. Reconnect the FI cable after the unit is re-configured as required.
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.
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.
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.
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. **Workaround**: Before performing an FI port configuration change, disconnect the FI cables on the unit. Reconnect the FI cable after the unit is re-configured as required.
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. **Workaround**: Reduce QoS precedence usage before upgrading to Release 10.2.
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.
wi01023541	**Lossless PFC mode**: In Lossless-PFC mode, regardless of flow control settings the port sends PFC frames on oversubscription. **Workaround**: You cannot configure the flow control modes for Lossless-PFC. Symm, Asymm, or Disabled flow control modes apply to Lossless (PAUSE) mode only.
wi01011829	**VRRP**: Intermittent. Error message might occur when enabling or disabling VRRP. **Workaround**: Reset the unit.

Reference number	Description
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.
wi01042491	**VLAN**: Adding one port to 1000 VLAN might take an extended period of time. **Workaround**: None, but adding multiple ports to a large number of VLANs takes time to complete.
wi01046311	**USB**: USB boot loading does not function with QoS lossless enabled. **Workaround**: Use ACLI to configure lossless mode.
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.
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. **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

Reference number	Description
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.
wi01086050	**Rear-port mode**: Fiber Fabric Interconnect cables are autonegotiation disabled, so flow control settings show as disabled or asymmetric.
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.
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

Reference number	Description
	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.
wi01102846	**SMLT/VLACP**: SMLT aggregation units become unresponsive and cannot be used after enabling VLACP on all SMLTs. **Workaround**: None. Do not enable VLACP.
wi01119196	**LACP/Transparent UNI**: LACP does not function on Transparent UNI ports.
wi01119204	**Transparent UNI**: Transparent UNI does not add other ports of the same LAG if the partner is down.
wi01119793	**ASCII script**: Auto download does not work from SFTP using ASCII script.
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
wi01127831	**VLACP**: VLACP may bounce under high CPU usage.
wi01144333	**SPBM over SMLT**: 100% CPU utilization and adjacencies bounce after reset a stack with SPBM over SMLT with 250 CVLANs. **Workaround**: None- Scaled environment. 250 CVLANS
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.

Reference number	Description
	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.
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.
wi01103003	**SMLT: SMLT / IST over Rear Ports**: Background traffic does not recover for approximately 80 seconds when disabling VLACP globally in an SMLT setup. **Workaround**: None
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	**Layer 2/SMLT**: Full traffic recovery may take up to 30 seconds when an NBU rejoins the stack in a highly scaled setup.
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.

Reference number	Description
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.
wi01140095	**Rear-ports**: Rear-ports speed mismatch (10 Mbps - 40 Gbps) if changing copper cable with fiber cable and boot. **Workaround**: Display issue only. Ports are running at 40 Gbps.
wi01142083	**Rear-ports**: Rear ports may not be up if inserting fiber Stack cable simultaneously in both peers after units are powered up (intermittent). **Workaround**: Wait 5 seconds after inserting cable in one unit prior to the second unit.
wi01142085	**Rear-ports**: Speed mismatch (1000 Mbps - 40 Gbps) may be seen when swapping rear-port fiber cable with copper cable (intermittent). **Workaround**: Display issue only.
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.
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 Unregistered Frames on IST ports.
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. **Workaround**: If seen, re-enable the shutdown ports and increase the RX threshold on both peers to higher values such as 50/100.
wi01157808	**SPBM/SMLT**: LACP port-mode is toggled from Advanced Mode to default after an SLT is deleted or modified. **Workaround**: When you modify LACP in an SMLT environment on either peer, check that the Advanced mode

Reference number	Description
	is still enabled on each peer and re-enable Advanced mode if it has been placed in default mode.
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.
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.
—	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.
wi01158262	**Multicast**: Multicast traffic is not forwarded to member ports when running in temporary base unit (TBU) with multicast-filter-mode enabled. When you enable multicast-filter-mode in a VLAN with IGMP snooping enabled, multicast traffic is not forwarded to member ports when running in TBU. **Workaround**: Use the `vlan igmp unknown-mcast-no-flood` command instead but take into account that this will also cut off control protocols like OSPF, RIP, and VRRP, as well as IPv6 and NetBEUI traffic.
wi01160393	**MDA**: A VSP 7000 MDA 10GBaseT port connected to Intel I35010G NIC may not come up at 10 Gbps. **Workaround**: Under investigation; a switch reset may resolve this issue in some cases.

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 3: Application mask and filter resource requirements

Application	Category	Masks required	Filters required
Broadcast ARP	Non QoS	1	1
DHCP Relay or DHCP Snooping	Non QoS	1	3
QoS interface group (untrusted and untrustedv4v6)	QoS	2	2
One QoS policy	QoS	1	Up to 200 if blocks are used
One QoS traffic profile set	QoS	Up to 8	Up to 75 if blocks are used
Port Mirroring (MAC-based or XY)	Non QoS	1	2
IPFIX	Non QoS	1	1
RIP	Non QoS	1	1
VRRP or OSPF	Non QoS	1	1
UDP Broadcast	Non QoS	1	1
IP Source Guard	Non QoS	1	11
FCoE redirect	Non QoS	3	3
SPBM	Non QoS	1	1
MAC security DA filtering (Bay Secure)	Non QoS	1	1 for each MAC address
Content-based forward to next hop	Non QoS	1 for each CF policy applied on each port.	1 for each mask.

Application	Category	Masks required	Filters required
CFM	Non QoS	2	1 for each mask
SLPP Guard	Non QoS	1	1

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.

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.

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
```