Avaya Virtual Services Platform 7000 Series Release Notes

Release 10.1
NN47202-400
Issue 02.02
October 2013

© 2013 Avaya Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. 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 its hardware and Software (“Product(s)”). 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. 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. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED 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 AUTHORIZED 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 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, 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”. 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, or hardware provided by Avaya. All content on this site, the documentation 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 that 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”). 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. 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. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: New in this release 7

Features 7

Fabric Interconnect Stacking 7

Media Dependent Adapter 8

Enterprise Device Manager (EDM) 8

802.1AB Link Layer Discover Protocol (LLDP) 9

802.1w Rapid Spanning Tree Protocol (RSTP) 9

802.1s Multiple Spanning Tree Protocol (MSTP) 9

802.3ad Link Aggregation Control Protocol (LACP) 10

ACLI audit log 10

Auto Unit Replacement (AUR) 10

BPDU Filtering 12

Configurable SNMP trap port 13

Configurable Asset ID 13

Configurable HTTP port 13

Disable Console port 13

Disable USB port 13

DNS client 13

Extended password history 14

Factory Default command 14

HTTP and HTTPs Web Server 14

Internet Group Management Protocol v1/v2 snooping and proxy 14

IP.CFG and IP.CFG extended support 15

IP Manager IPv6 and SSH support 16

IPv6 support for IP manager 16

Logout ACLI enhancement 17

MLT/DMLT/LAG scaling 17

New Unit Quick Configuration (NUQC) 17

QoS Agent operational mode 18

QoS classifiers and classifier blocks 18

QoS DSCP mutation 18

QoS IP, L2 filter, and system options 19

QoS Lossless mode 20

QoS Queue Set support 20

QoS Traffic Profile filter set 20

Traffic Profile metering 21

QoS VLAN range support 21

RADIUS management 21

Reload command 22

RMON Ethernet history and statistics 22

Secure File Transfer Protocol (SFTP) 23

Secure Shell protocol (SSH) 23

Show boot command 23

Simple Network Time Protocol (SNTP) support 23

SNMP trap support ... 24
Stack Forced Mode ... 24
Stack Health Check ... 24
Stack Health Monitoring and Recovery ... 24
Stack Loopback Tests ... 24
Stack Monitor ... 25
Stack Port Counters ... 25
TACACS+ ... 26
Terminal Mode Permanent Setting ... 26
Terminal Security Mode ... 26
Total System Uptime ... 26
Traceroute ... 26
USB support ... 27
Unified Authentication ... 27
Virtual Link Aggregation Control Protocol ... 27
VLAN scaling ... 28
Other changes ... 28
Chapter 2: Important notices ... 29
Warnings and important notices ... 29
File names for this release ... 31
Software and hardware capabilities ... 32
Supported browsers ... 34
Upgrading switch software using ACLI ... 34
Upgrading switch software using EDM ... 36
Supported standards, MIBs, and RFCs ... 39
Standards ... 39
RFCs and MIBs ... 39
Chapter 3: Resolved issues ... 43
Resolved issues for Release 10.1 ... 43
Chapter 4: Known issues and limitations ... 45
Known issues ... 45

Chapter 1: New in this release

The following sections detail what is new in Avaya Virtual Services Platform 7000 Series Release 10.1

VSP 7000 hardware:

The following table lists and describes new hardware supported in VSP 7000 Series Release 10.1.

Hardware	Description
Adaptors and cables	
AL7018001–E6	VSP 7000 Fabric Interconnect cable 0.6M.
AL7018002–E6	VSP 7000 Fabric Interconnect cable 1.5M.
AL7018003–E6	VSP 7000 Fabric Interconnect cable 3.0M.
AL7018004–E6	VSP 7000 Fabric Interconnect cable 5.0M
AL7018005–E6	VSP 7000 Fabric Interconnect cable 10.0M
7008XLS	VSP 7000 Media Dependent Adaptor — provides 8 SFP+ ports.
7008XT	VSP 7000 Media Dependent Adaptor — provides 8 10GBASE-T ports.

Features

See the following sections for information about new features.

Fabric Interconnect Stacking

The VSP 7000 Series with Release 10.1 supports Fabric Interconnect (FI) Stacking. You can Fabric Interconnect up to eight VSP 7000 Series switches, providing connectivity for up to 256 ports in one virtual chassis. Fabric Interconnect allows for flexible, scalable, and redundant deployments of multiple units supporting up to 5120 Gbps of bandwidth between units. This high speed, low latency connection is useful for Data Centre deployments where Fabric Interconnect can address the requirements of East-West traffic between adjacent racks within the Data Centre, without the added latency or higher costs associated with sending traffic North-South to transit adjacent racks.

Each VSP 7000 has a pair of FI-up and FI-down ports, which for Fabric Interconnect Stacking should be considered as one logical connection. To create a Fabric Interconnect Stack, you can connect switch units using a pair FI cables which connect the pair of FI-up ports on one

unit to the FI-down ports on another unit. Once adjacency is established across units, the Fabric Interconnect Stack or virtual chassis is operational. You can efficiently manage a virtual fabric as a single unit through the use of a Stack IP address.

The VSP 7000 supports the following Fabric Interconnect cables. (Avaya recommends to purchase and install cables in pairs):

Order Code	Description
AL7018001–E6	VSP 7000 Fabric Interconnect 0.6m
AL7018002–E6	VSP 7000 Fabric Interconnect 1.5m
AL7018003–E6	VSP 7000 Fabric Interconnect 3m
AL7018004–E6	VSP 7000 Fabric Interconnect 5m
AL7018005–E6	VSP 7000 Fibre Fabric Interconnect 10m

Media Dependent Adapter

A Media Dependent Adapter (MDA) is a field replaceable expansion module that provides additional capability on the VSP 7000. Each VSP 7024XLS supports the installation of one MDA. With Release 10.1, two types of MDA are supported which provide eight additional ports of either 10 Gigabit SFP+ or 10 Gigabit BaseT.

It is recommended to insert, swap, or remove the MDA when the switch is powered down, otherwise the switch does not detect the MDA. With Fabric Interconnect Stacking, a unit can be taken out of service to insert, swap, or remov an MDA without impacting the other units with the Stack. Future software will support hot insertion, hot swap, and hot removal of MDAs in units.

The VSP 7000 supports the following MDAs with Release 10.1:

Order Code	Description
AL7000MS1–E6	VSP 7008XLS MDA 8 SFP+ ports
AL7000MT1–E6	VSP 7008XT MDA 8 10GBASE-T ports

Enterprise Device Manager (EDM)

Enterprise Device Manager (EDM) is an embedded element management and configuration application you can use to configure and manage the switch or Fabric Interconnect Stack. EDM is a Web-based graphical user interface that you can access through a standard web browser.

802.1AB Link Layer Discover Protocol (LLDP)

The VSP 7000 supports IEEE 802.1AB, also known as Link Layer Discovery Protocol (LLDP). With LLDP, local area network (LAN) stations can share station capability data with each other, which permits the discovery of physical network topology.

802.1w Rapid Spanning Tree Protocol (RSTP)

802.1w Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1w standard, is an evolution of the 802.1D standard more than a revolution. The 802.1D terminology remains primarily the same, so users familiar with 802.1D can rapidly configure the new protocol comfortably. RSTP provides significantly faster spanning tree convergance after a topology change by introducing new convergence behavious and bridge port roles.

RSTP by default takes 6 seconds (3 x Hello times, which are 2 seconds each) to respond to a topology change on the network compared to 30 to 50 seconds required for STP. Each RSTP instance on the switch can include one or more VLANs, and RSTP is backwards-compatible with standard STP.

802.1s Multiple Spanning Tree Protocol (MSTP)

Multiple Spanning Tree Protocol (MSTP), originally defined in IEEE 802.1s defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.

MSTP allows formation of MST regions that can run multiple MST instances (MSTI). Multiple regions and other STP bridges are interconnected using one single common spanning tree (CST).

MSTP includes all spanning tree information in a single BPDU format, reducing the number of BPDUs required on a LAN to communicate spanning tree information for each VLAN, and ensuring backward compatibility with RSTP (and in effect, classic STP too). MSTP encodes additional region information after the standard RSTP BPDU as well as a number of MSTI instances. Each of these MSTI configuration messages conveys the spanning tree information for each instance.

MSTP is fully compatible with RSTP devices, an MSTP BPDU can be interpreted by an RSTP device as an RSTP BPDU. This allows compatibility without configuration changes, and allows any RSTP device outside of an MSTP region to see the region as a single RSTP device.

802.3ad Link Aggregation Control Protocol (LACP)

Link Aggregation Control Protocol (LACP) as defined by IEEE 802.3ad provides a standard means to manage switch port memberships to Link Aggregation Groups (LAGs). Link Aggregation is a method of combining one or more physical network links into a single logical link. Link Aggregation increases the capacity and availability between devices (both switches and end stations). Without manual overrides, an appropriate set of LAGs is automatically configured and individual links are allocated to those groups.

ACLI audit log

ACLI audit log provides tracking for all ACLI commands.

A special area of NVRAM on the switch is reserved to store ACLI command history. When you enable the ACLI audit log, every time you issue an ACLI command, the switch generates and stores an audit message.

Disable ACLI audit log:

The ACLI audit log defaults to automatically record a history of all ACLI commands entered using the console port (serial port), Telnet, and Secure Shell (SSH). A configuration option is available in Release 10.1 to disable ACLI audit logging.

Erasable ACLI audit log:

You can erase the contents of the ACLI audit log on a switch, for use in situations that require the log contents to be cleared. For example, you can clear the ACLI audit log contents on switches being decommissioned.

To prevent the ACLI audit log contents from being erased, you can apply the `noerase` function. This function can be applied once on a switch and is not reversible.

Auto Unit Replacement (AUR)

Automatic Unit Replacement (AUR) encompasses a number of features that can provide plug and play unit replacement for VSP 7000 units running in a Fabric Interconnect Stack.

The AUR function refers specifically to the ability to retain the configuration (CFG) image of a unit in a Fabric Interconnect Stack when you replace a unit with a like for like unit. The AUR configurations for each unit in the Fabric Interconnect Stack are maintained on the operating Base Unit. The AUR configuration is applied to an operating replacement unit connected to the Fabric Interconnect Stack.

You can enable or disable AUR using the ACLI `[no] stack auto-unit-replacement enable` command, or using EDM.

Auto Unit Replacement Disable Synchronization

AUR Disable Synchronization provides the ability to disable synchronization of the configuration files to the Base Unit when AUR is operational. This allows you greater control over the synchronization of configuration files in AUR to the Base Unit. For example, you can enable AUR synchronization to mirror AUR configurations to the Base Unit, then disable synchronization once synchronized, so that a known good AUR configuration is stored in the Base Unit memory.

You can disable or enable AUR synchronization using the ACLI `stack auto-unit-replacement config [disable | enable]` command, or using EDM.

Auto Unit Replacement Forced Synchronization

AUR Forced Synchronization provides the ability to force synchronization of an AUR configuration file stored in the Base Unit memory to a specific unit.

You can manually synchronize the configuration from a unit in the Fabric Interconnect Stack to the Base Unit using the ACLI `stack auto-unit-replacement config save unit <n>` command, or using EDM. You can restore the configuration to a specific unit in the Fabric Interconnect Stack using the ACLI `stack auto-unit-replacement config restore unit <n>` command, or using EDM.

Auto Unit Replacement MAC address

AUR MAC address provides the ability to display and remove entries from the Automatic Unit Replacement (AUR) cache. The Fabric Interconnect Stack stores the MAC addresses of all units that are or have been a member of the stack. AUR checks the MAC addresses when a unit joins the stack to determine if AUR needs to be applied. Displaying and then removing an address from the AUR cache can be useful if you are trying to demonstrate AUR/AAUR/DAUR functionality, but do not have a replacement unit, or if you are trying to force a unit to be automatically refreshed. Before you can remove the MAC address of a unit from the AUR cache, the unit must be disconnected from the Fabric Interconnect Stack before you issue the remove command.

You can display the AUR MAC address cache using the ACLI `stack auto-unit-replacement mac-addresses` command. You can remove a unit MAC address from the AUR cache using the ACLI `stack auto-unit-replacement remove unit <n>` command.

Agent Auto Unit Replacement (AAUR)

Agent Auto Unit Replacement (AAUR) is a supplementary AUR function to ensure that all units in a Fabric Interconnect Stack are operating using the same agent software image. AAUR inspects units joining a Fabric Interconnect Stack and upgrades or downloads the agent software image to any unit operating a different agent software image than the Base Unit (BU). AAUR is enabled by default to ensure that the same agent software operates on all units within the Fabric Interconnect Stack.

You can disable or enable AAUR using the ACLI `[no] stack auto-unit-replacement-image enable` command, or using EDM.

Diagnostic Auto Unit Replacement (DAUR)

Diagnostics Auto Unit Replacement (DAUR) is a supplementary AUR function to ensure that all units in a Fabric Interconnect Stack are operating using the same diagnostics software image. DAUR inspects units joining a Fabric Interconnect Stack and upgrades or downloads the diagnostics software to any unit operating a different diagnostic software image than the Base Unit (BU). DAUR is enabled when AAUR is enabled and ensures that the same diagnostics software operates on all units within the Fabric Interconnect Stack.

BPDU Filtering

The Bridge Protocol Data Unit (BPDU) Filtering feature allows the network administrator to control how Spanning Tree BPDUs are controlled within a network to help prevent against malicious network attacks. The main purpose of a Spanning Tree is to eliminate loops in a network. A bridge that participates in the Spanning Tree Protocol exchanges information through configuration messages known as BPDUs. Based on the BPDU information all the bridges select a single bridge with the best bridge ID as the Root. This process is called the Root selection process. When a new bridge joins the network or an existing bridge leaves the network the Root selection process repeats and the new Root is selected due to the network change.

BPDU Filtering provides network protection by enabling:

- Blocking of unwanted Root selection processes when an edge device is added to the network. This prevents unknown devices or malicious users from altering the existing Spanning Tree topology.
- Block the BPDU Flooding of the switch from an unknown device. BPDU Filtering can be enabled on a per port basis or across all ports at once. Each port has its own timer configurable between 10 seconds and 65535 seconds to determine how long a port will be disabled if a BPDU is received on that port. If the timer is set to 0 and a BPDU is received on that port, the port is administratively disabled until it is explicitly enabled by an authorized network administrator.

When a port receives a BPDU and BPDU Filtering is enabled, the following action occur:

- The port is immediately placed in the operational disable state.
- A SNMP rap and a log message is generated. The log message is “• BPDU received on port with BPDU Filtering enabled. Port X has been disabled”.
- The port timer starts and the port stays operationally disabled until the port timer expires. If the timer is disabled or the switch resets before the timer countdown expires, the port temporarily disabled by the BPDU Filter application stays in a disabled state.

If you disable BPDU Filtering while the timer is running, the timer countdown stops and the port temporarily disabled by the BPDU Filter application stays in a disabled state. In this situation, If the BPDU Filtering disabled a port, you must manually enable the port to return the port to normal operating mode.

Configurable SNMP trap port

You can change the SNMP trap port from the default UDP port 162, to between 1025 and 65535 using an ACLI command. You can restore the SNMP trap port to UDP port 162 using an ACLI default SNMP port command.

Configurable Asset ID

You can define an Asset ID to provide inventory information for the switch, stack, or each unit in a stack. An Asset ID consists of an alphanumeric string of up to 32 characters in length. An Asset ID is useful for recording your company specific asset tracking information, such as an asset tag attached to the unit.

Configurable HTTP port

You can change the HTTP port from the default port 80 to between 1025 and 65535 using an ACLI command. You can specify a different port for web browsers to use to connect to the switch, and changing the port can also improve security. To restore the HTTP port to port 80, use an ACLI default HTTP port command.

Disable Console port

You can disable local management ports on the switch for improved security. You can disable or enable the serial console port on the VSP 7000 using the ACLI `[no] serial-console [unit <n>] enable` command.

Disable USB port

You can disable local management ports on the switch for improved security. You can disable or enable the USB ports on the VSP 7000 using the ACLI `[no] usb [unit <n>] enable` command.

DNS client

You can configure IPv4 and IPv6 DNS servers, enabling the VSP 7000 to perform domain name lookups. Configuring DNS servers allows you to use ACLI commands such as ping, telnet, SSH, TFTP with host names rather than specific IP addresses.

Extended password history

The VSP 7000 supports password history and extended password security capabilities. Password history and security is automatically enabled when running the secure (SSH) software image.

Factory Default command

You can use the ACLI `restore factory-default` command to return the switch to default configuration. You can also include a `-y` parameter for the command to execute immediately without requesting confirmation.

HTTP and HTTPs Web Server

The VSP 7000 supports management of the switch through HTTP and HTTPs using the Enterprise Device Manager (EDM).

Internet Group Management Protocol v1/v2 snooping and proxy

The VSP 7000 supports Internet Group Management Protocol (IGMP) v1/v2 snooping and proxy capabilities. With IGMP, IP multicast routers can learn the existence of multicast group members connected directly to router subnets. Hosts can use IGMP to register group members to a local querier router.

To maintain multicast traffic, the VSP 7000 supports the following:

- IGMPv1: Routers using IGMPv1 periodically send host membership queries to connected local subnets to inquire if hosts attached to the subnets are interested in joining IP multicast groups.
- IGMPv2: With IGMPv2, the mechanism of implementing a host leave message is added to the IGMPv1 function. Using this mechanism, instead of routers sending multiple queries to determine that hosts have left an IP multicast group, the hosts leaving the group can send a leave message to the router.
- IGMP snooping and proxy: With IGMP snooping enabled on a VLAN, the switch forwards multicast group data to only those VLAN ports that are members of that group. This process prevents the flooding of hosts not participating in the group, which can result in unnecessary bandwidth consumption.

IP.CFG and IP.CFG extended support

IP.CFG allows you to rapidly pre-stage Avaya switches that support a USB device and the IP.CFG function. If a USB device with IP.CFG is installed in the VSP 7000, when the switch boots in a factory default state, it scans for the existence of the IP.CFG file on a USB storage device. If the file exists, the switch processes the information in the file to pre-stage the switch.

You can specify one or more of the following parameters in the IP.CFG file:

Table 1: IP.CFG parameters

Parameter	Description
IP <A.B.C.D>	Specifies the IP address for the switch. Example, 192.168.22.1
Mask <A.B.C.D>	Specifies the network mask. Example, 255.255.255.0
Gateway <A.B.C.D>	Specifies the default gateway, Example, 181.30.30.254
SNMPread <string>	Specifies the SNMP read community string. Example, public
SNMPwrite <string>	Specifies the SNMP write community string. Example, private
VLAN <number>	Specifies the management VLAN ID. Example, VLAN 1
USBdiag <string>	Specifies the file name of the diagnostic image to load from the USB device. Example, vsp7000/7000_101060.bin
USBascii <string>	Specifies the file name of the ASCII configuration file to load from the USB device. Example, customer1.cfg
USBagent <string>	Specifies the file name of the runtime agent image to load from the USB device. Example, vsp7000/7000_101000.img
NEXTIP, NEXTMask, and NEXTGateway	Specifies IP addresses, network mask, and gateway to be used once the switch is booted.

The IP.CFG file loads information from the configuration file in order of precedence and any lines commencing with a # character are treated as a comment and not processed.

The following example IP.CFG file applies the indicated IP addresses and gateways and configuration file if you boot the VSP 7000 in factory default configuration.

Note:

If the ASCII configuration file contains IP address information, since it is specified after the IP address information in IP.CFG, the IP Address information from the ASCII configuration file takes precedence.

```
#Example IP.CFG
IP 172.16.1.80
Mask 255.255.255.0
Gateway 172.16.1.1
USBascii VSP7000rack.txt
```

Important:

To use the IP.CFG capability, the switch must be in default configuration (either factory defaulted or new out of box) and a USB storage device with the IP.CFG file in the root directory must be present. The switch attempts to read the IP.CFG present within the first three minutes of switch operation. If a console is connected to the switch during the boot process and you require IP.CFG to operate, then DO NOT attempt to access the switch for at least three minutes. This is necessary to give the switch sufficient time to detect and process IP.CFG functions.

The system does not display a message to indicate the IP.CFG file progress, you need to connect to the switch after 3 minutes of booting to verify the IP.CFG operation. You can typically confirm the successful download of IP.CFG by using the ACLI `show ip` command. If the USB IP.CFG file download succeeded, all parameters read from the file show are present in the switch and part of the runtime configuration.

IP Manager IPv6 and SSH support

You can limit access to the management features of the VSP 7000 by specifying the IP addresses allowed to access the switch. IP Manager support is expanded to support Secure Shell (SSH) and IPv6.

IPv6 support for IP manager

This feature provides management support for the VSP 7000 through IPv6. Functionality includes IPv6 host access to the switch, as well as access to a number of management functions over IPv6.

The following functions support IPv6 addressing:

- DNS client
- HTTP/EDM
- RADIUS servers
- SFTP

- SNMP
- SNTP
- SSH client
- IP Management address
- Syslog
- Telnet
- TFTP

Logout ACLI enhancement

The logout command functions differently than the exit command. The ACLI `logout` command provides a disconnect from the switch similar to the logout command on a Linux or Unix system. If you run the command when connected through the Console, the session returns to the login or banner screen. If you run the command when connected through Telnet or SSH, the session terminates and closes the current session.

The logout and exit command help messages are updated, logout description is “Exit from the EXEC and end the current session”, exit description is “Exit from the current context”.

MLT/DMLT/LAG scaling

MultiLink Trunking (MLT), Distributed MultiLink Trunking (DMLT), and Link Aggregation Groups (LAG) scaling supports up to 32 trunk groups with up to 8 links per trunk for MLT, DMLT, and LAG.

New Unit Quick Configuration (NUQC)

You can use the New Unit Quick Configuration (NUQC) feature to create a configuration template, which is applied to any new unit joining the Fabric Interconnect Stack. NUQC can configure the VLAN IDs, port speed, duplex mode, PVID, tagging, and other port specific information for the new unit when joining a Fabric Interconnect Stack.

NUQC is disabled by default. Once enabled NUQC tracks the MAC addresses of all units in the stack in order to detect new units.

You can create a configuration template using the ACLI `quickconfig start-recording` command. You can end the recording by entering a period (.). When recording commands, you can use the dollar symbol ($) to indicate the unit number.

Example recording script:

```
VSP7024XLS# quickconfig start-recording
ena
```

```
config terminal
vlan ports $/1-2,$/5-24 tagging enable
vlan members add 2 $/1-2
vlan ports $/1-2 pvid 2
vlan members add 3 $/5-24
vlan ports $/5-24 pvid 3
interface fastEthernet all
spanning-tree port $/1-24 learning disable
exit
.
```

QoS Agent operational mode

You can enable or disable the QoS Agent using ACLI. Disabling the QoS Agent allows you to easily and temporarily disable all QoS settings for debugging system configuration issues.

QoS classifiers and classifier blocks

You can use classifiers and classifier blocks with a policy to direct how the system handles traffic.

You can combine packet classifier elements into classifiers, and you can group one or more classifiers into classifier blocks.

You can configure packet, IP, Layer 2, and system classifier elements.

Traffic Profile filter set support provides the recommended configurations for QoS or filter capabilities.

QoS DSCP mutation

When you configure a trusted QoS interface, the default is that the IPv4 traffic received on the trusted interface is remarked at the Layer2 level. The 802.1p user priority value is updated based on the DSCP value in the packet at inggress as per the DSCP-to-CoS mapping data. The remarked CoS value is used for egress queuing on the switch and can be used for downstream packet processing

QoS DSCP mutation supports the remarking of DSCP values in conjunction with trusted interface processing, without the need to utilize filters, ACLs, or Traffic Profiles. With DSCP mutation, the switch can modify the DSCP value of the packet based on the mapping in the DSCP-to-COS mapping table. The DSCP value updates if the DSCP egress value differs from the ingress value in the mapping table.

QoS IP, L2 filter, and system options

VSP 7000 Release 10.1 provides greater flexibility in QoS options.

Qos Layer2 criteria:

- Source MAC address/mask
- Destination MAC address/mask
- VLAN ID range
- VLAN tag
- EtherType
- Packet type
- 802.1p priority values

QoS IPv4 criteria:

- 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 flags
- TCPv4 control flags
- IPv4 options

QoS IPv6 criteria:

- IPv6 source address/mask
- IPv6 destination address/mask
- 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 system criteria:

- unknown IP multicast
- known IP multicast
- unknown non-IP multicast
- known non-IP multicast
- non-IP packet
- unknown unicast packet

QoS Lossless mode

Quality of Service (QoS) Lossless mode is critical in data center applications, where reliable data transfer is more important than enhanced throughput. With Lossless mode, when a port receives volumes of traffic greater than egress port bandwidth, the port sends flow control (pause) frames to all sending ports until the congestion on the egress port is reduced to below the critical threshold.

Important:

Avaya recommends you to use the queue set configuration default of 2 queues when operating in Lossless mode.

QoS Queue Set support

You can select from 8 different egress queue sets, supporting from 1 to 8 egress queues, to be used for packet queuing and scheduling at egress. You can also specify the amount of buffer sharing that occurs across ports. Egress queue set selection and buffer sharing allows you greater flexibility to tune the egress queue configuration and buffer utilization of the switch to the types of traffic and congestion that can occur on your network.

VSP 7000 Release 10.1 default queue configuration is 2 priority queues with a medium level of buffer sharing.

QoS Traffic Profile filter set

A filter set is an ordered list that contains classifiers, classifier blocks, and the associated action and meter criteria to be applied to traffic that matches the classifier data. VSP 7000 Release 10.1 introduces Traffic Profile filter set support that allows you to construct and apply a series of policies (classifiers/actions/meters) to an interface. Traffic Profile filter sets support

advanced traffic identification and flexible metering options on a per-policy and per-classifier basis. You can modify the set while it is in use.

Traffic Profile filter set support provides improvements over Access Control List (ACL) support. Avaya recommends using Traffic Profile filter set to configure QoS or filter capabilities.

Traffic Profile metering

You can use policy-based and classifier-based metering modes with Traffic Profile Filters. Traffic metering can be applied to individual classifiers, blocks of classifiers and individual block members. Policy-based metering associates a unique meter with each policy that comprises the filter set.

There are two types of policy-based metering:

- uniform metering — each meter has the same characteristics derived from the filter set instance definition.
- individual metering — each meter has unique characteristics derived from the individual classifier or master block classifier member associated with the filter set policy.

QoS VLAN range support

VSP 7000 Release 10.1 allows you to specify a full range of VLANs when using ACLI and QoS Traffic Profiles or other filtering capabilities.

RADIUS management

Remote Authentication Dial-In User Service (RADIUS) is a client and server system that helps secure networks against unauthorized access by providing authentication, authorization, and accounting for network access.

The VSP 7000 supports the ability to authenticate a user who wants to access the switch for management purposes. RADIUS Management can be enabled or disabled separately for console, Telnet, or EDM access. When enabled, the user is prompted for a username and password when attempting to connect to the switch. The username and password are verified against the RADIUS Server, and if successful, the user is permitted access.

RADIUS management is disabled by default. If enabled, Avaya recommends you to configure two RADIUS servers for improved reachability.

RADIUS management accounting

RADIUS management accounting provides the ability to record the management login activities to the switch. The switch returns an authentication message to the RADIUS server

for logging purposes. The accounting records generate when you access the switch through the console, Telnet, SSH, or EDM, or when you disconnect the session by logoff or timeout.

RADIUS password fallback

The RADIUS password fallback feature lets the user log on to the VSP 7000 by using the local password if the RADIUS server is unavailable or unreachable for authentication.

RADIUS password fallback is disabled by default.

Reload command

The ACLI `reload` command provides you with a configuration rollback mechanism to prevent loss of connectivity to a switch, typically for remote configurations. The reload command allows you to temporarily disable the autosave feature for a specified time period (1 to 60 minutes). Once the reload timer expires, the switch reboots and reloads the last saved configuration. This allows you to make a number of configuration changes on the remote switch without affecting the current saved configuration.

As a result, if you lose connectivity while remotely configuring the switch, the last saved configuration is reloaded at the end of the configured time period, and you regain the switch connectivity. During the interval when autosave is disabled by the reload command, you must use the `copy config nvram`, `write mem`, or `save config` command to force a manual save of your configuration.

To abort the switch reload before the timer expires, you can enter the `reload cancel` command.

RMON Ethernet history and statistics

Remote Monitoring (RMON) specifications define a set of statistics and functions to collect and exchange network information. The VSP 7000 supports RMON2 level of instrumentation for 4 groups. VSP 7000 Release 10.1 RMON agent capabilities are enhanced to provide both historical and statistical group information.

RMON history records periodic samples from a network, gathered in time intervals referred to as buckets. By default, RMON gathers history information based on 50 buckets, with each bucket supporting a sample interval of 30 minutes.

RMON statistics allows the VSP 7000 to report on the statistics group, to provide information such as broadcast and multicast packets and error statistics about cyclic redundancy check (CRC) alignment errors and collisions.

Secure File Transfer Protocol (SFTP)

For secure (SSH) software images Secure File Transfer Protocol (SFTP) supports the downloading of agent and diagnostic image files, the transfer of configuration files (binary or ASCII) to and from a SFTP server. SFTP allows secure transfer of files between a switch or Fabric Interconnect Stack and an SFTP server that uses SFTP with SSH version 2. Enabled by default, SFTP is available through ACLI and EDM.

Secure Shell protocol (SSH)

Secure Shell (SSH) protocol provides secure network services over an insecure network and can be used as a replacement for Telnet, when secure access to the Avaya Command Line (ACLI) interface is required.

Secure Shell client

The SSH client provides the ability to initiate a SSH session from a switch to another device (in the same way you can Telnet to another device in the network). By using SSH rather than Telnet, a secure session is established between devices which significantly reduces the ability to compromise the management session. The ability to use SSH is present only on switches running the Secure (SSH) image, and is available only through ACLI. SSH Client uses SSH version 2 and supports DSA, RSA and password based authentication.

Show boot command

You can display the currently loaded and operational software status for both agent and diagnostic loads as well as the status of any loaded software licenses (if applicable). The ACLI `show boot` command allows you to view the status of the agent and/or diagnostic images.

The `show sys-info` and `show tech` commands are enhanced to display the loaded and operational diagnostic and agent software as well as the currently loaded and operational software licenses (if applicable).

Simple Network Time Protocol (SNTP) support

The Simple Network Time Protocol (SNTP) feature allows the VSP 7000 to synchronize the local Real Time Clock to Universal Coordinated Time (UTC) to an accuracy within 1 second. This feature adheres to the RFC 2030.

If you run SNTP, the system synchronizes with the configured SNTP server (primary then secondary) at during boot and at user-configurable periods thereafter (the default

synchronization interval is 24 hours). The first synchronization does not occur until network connectivity is established.

SNTP is disabled by default. SNTP also supports the ability to configure time zones, Daylight Savings Time and recurring Daylight Savings.

SNMP trap support

SNMP trap enhancements provide the option to enable or disable notifications for objects on specific interfaces, as well as globally. All SNMP traps are enabled by default, globally and per interface, but you can modify them according to your requirements, using SNMP trap notification control.

Stack Forced Mode

Stack Forced Mode is recommended when your system is a VSP 7000 Fabric Interconnect Stack of 2 units. Stack Forced Mode ensures that if one of the 2 units fails, the remaining standalone unit can maintain the Stack IP Address. Additionally Stack Force Mode ensures that if the non Base Unit is replaced in a Stack of 2 units, that AUR and it's associated functions operate as expected

Stack Health Check

The Stack Health Check feature provides information on the state of each unit in the Fabric Interconnect Stack, as well as the health of the Fabric Interconnect cables. Stack Heath Check also identifies which unit is operating as the Base Unit (BU) or Temporary Base Unit (TBU). Stack Health Check runs a high-level test to monitor the FI port status for each unit, as well as determining the number of units in a Fabric Interconnect Stack.

Stack Health Monitoring and Recovery

Stack Health Monitoring and Recovery automatically provides a robust switch discovery mechanism for Fabric Interconnect Stack operation. Additional monitoring and logging information produced by switches in the Fabric Interconnect Stack ensure that more information is available for troubleshooting if any stack related issues occur.

Stack Loopback Tests

You can test your Fabric Interconnect (FI) ports and FI cables by using the Stack Loopback Test. The Stack Loopback Test is useful to determine whether the source of the problem is a

defective Fabric Interconnect (FI) cable or a damaged FI port. The test can help prevent unnecessarily sending switches for service. Two types of loopback tests exist. The internal loopback test verifies that the FI ports are functional. The external loopback test checks if the FI cables are functional.

Important:

Stack Loopback Tests provide limited functionality in Release 10.1. For more information, see the known issues section.

Stack Monitor

Many complex systems are monitored and controlled through Ethernet networks. When these systems are connected to stackable switches, it becomes more important to be able to actively monitor the health of switches in a Fabric Interconnect Stack. The Stack Monitor feature actively monitors the number of units in a stack and generates SNMP traps and log messages if the number of units changes from the configured value.

Each time the number of units in a stack changes, the trap sending timer is reset and the current number of stack units is compared with the configured number of stack units. If it is not equal, the switch sends a trap and log a message to Syslog. The traps are sent from a standalone unit or the Base Unit (BU) of the stack. When the trap sending timer reaches the configured number of seconds for when traps are sent, the switch sends a trap and logs a message to Syslog and restarts the trap sending timer. The Syslog message is not be repeated unless the stack configuration changes. This prevents the log from being filled with stack configuration messages.

Stack Monitor is disabled by default. When this feature is enabled on a Fabric Interconnect Stack, the current stack size is logged and used as the expected stack size. Alternatively, you can choose a different value and configure it after enabling the feature. You can configure Stack Monitor using ACLI or EDM.

Stack Port Counters

The stack port counters measure packet statistics for the Fabric Interconnect ports of a unit. You can view or clear the Fabric Interconnect Stack port counter statistics using ACLI.

Important:

The stack counters measure the size of packets received and transmitted on FI-up and FI-down ports. The size of the packets reported on the FI ports is greater than traffic received on front panel ports since additional header information is added to the packets while transiting the Fabric Interconnect Stack. Also the packet counter for the FI ports includes traffic received and transmitted on the ports used for Fabric Interconnect Stack operation.

TACACS+

TACACS+ provides access control for the management of the switch through one or more centralized TACACS+ servers as an alternative to RADIUS. Additionally, TACACS+ provides separate authentication, authorization and accounting services.

Terminal Mode Permanent Setting

Terminal Mode Permanent Setting saves terminal settings across login sessions. Retaining the terminal settings allows for easier use of scripts to configure or poll the switch.

Terminal Security Mode

Terminal Security Mode enables the switch console port to operate in a more secure mode of operation. When terminal security mode is enabled, the VSP 7000 sends echo characters to the terminal device. If the switch detects a lack of echo response characters, the current console session logs out.

You can configure Terminal Security Mode using the ACLI `terminal serial-security` command. You can display the status of the Terminal Security Mode using the ACLI `show terminal serial-security` command.

Total System Uptime

Total System Uptime tracks the total time the switch has operated rounded to the nearest day. Total System Uptime provides a record of the total operating time of the switch, similar to how an odometer records the total distance a vehicle has travelled.

You can display the Total System Uptime using the ACLI `show system total-up-time` command.

Traceroute

You can use the traceroute command as a diagnostic tool to identify various IP devices on the network and interpret delays or errors.

Traceroute sends a sequence of Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host. Determining the intermediate routers traversed by increasing the time-to-live (TTL) parameter of each successive set of packets sent. The first set of packets sent have a TTL 1 and report on reachability of the first routing device. The next

set has a TTL value of 2, so that the second routing device is reported. This process continues until the destination host receives the packets and returns an ICMP Echo Reply message.

USB support

VSP 7000 Release 10.1 provides support for the USB front panel port. You can use the USB port to connect USB storage devices to the switch to transfer files and software images.

The following USB functions are also supported:

- show usb host-port
- show usb-files (includes subdirectory support
- USB ASCII config support
- USB load-on-boot

Unified Authentication

VSP 7000 Release 10.1 supports Unified Authentication. With Unified Authentication you can manage one set of local usernames and passwords for switches, whether the units are operating as standalone switches or operating as part of a Fabric Interconnect Stack.

The Unified Authentication mechanism approach simplifies the design. Using the current ‘cli password’ and ‘username’ commands, the same set of read-write/read-only username, password, and authentication type applies to the Fabric Interconnect Stack as well as each standalone switch. The VSP 7000 obsoletes and clears the switch passwords and username; so whether the unit is operating in either standalone or Fabric Interconnect Stacked mode it always uses the Fabric Interconnect Stack (aka Unified Authentication) password and username.

Note:

You must properly configure the management IP address of the switch or Fabric Interconnect Stack before configuring RADIUS or TACACS+ authentication. Otherwise, you can be locked out of the system since the server providing authentication cannot be reached.

With Unified Authentication, when you configure RADIUS or TACACS+ on a Fabric Interconnect Stack, the authentication type applies to each switch in the stack configured with a standalone IP address.

Virtual Link Aggregation Control Protocol

In many enterprise networks, it is a requirement for a trunk link to fail over to the other link within a sub-second interval if there is a failure in the link between the local and the remote

end points. This requirement can be met if the network can inform both ends of the link in the event of a communication loss. Virtual Link Aggregation Control Protocol (VLACP) is used to detect end-to-end failure by propagating link status between ports that are logically connected point-to-point, either directly or indirectly across an intermediate network.

Two additional VLACP message types (DOWN and HOLD) are supported to allow VLACP to better detect and respond to certain one-way communication failures. The addition of the VLACP DOWN sub-type enables one switch to provide notification to the other switch of a one-way communication.

You can configure the VSP 7000 to receive and process VLACP HOLD messages. A remote device can generate a VLACP HOLD PDU to indicate that the ports are not ready to receive traffic. This configuration can ensure that all VLACP enabled ports on the remote switch have sufficient time to be ready to receive, and forward ingress traffic before the link is in service. You can enable this feature by configuring a positive value for VLACP HOLD time that matches the remote device.

VLAN scaling

VSP 7000 Release 10.1 supports up to 1024 concurrent VLANs with VIDs in a range from 1 to 4094. With VLAN scaling, ACLI is enhanced to allow add/delete/membership operations for a group of VLANs, allowing you to perform faster configuration of a large number of VLANs. If you perform multiple VLAN operations using the new commands, you must configure the VLAN configuration control to flexible, unless the port is “tagged” (tagging is tagAll or untagePvidOnly).

Other changes

See the following sections for information about changes that are updates to previously existing information.

Upgrading the software

Upgrading switch software using ACLI on page 34 is updated.

Chapter 2: 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.

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.

Caution:

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.

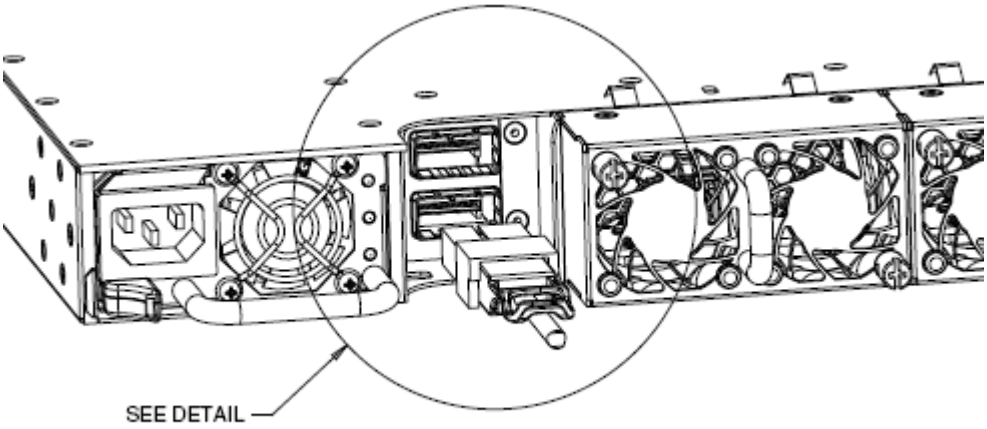
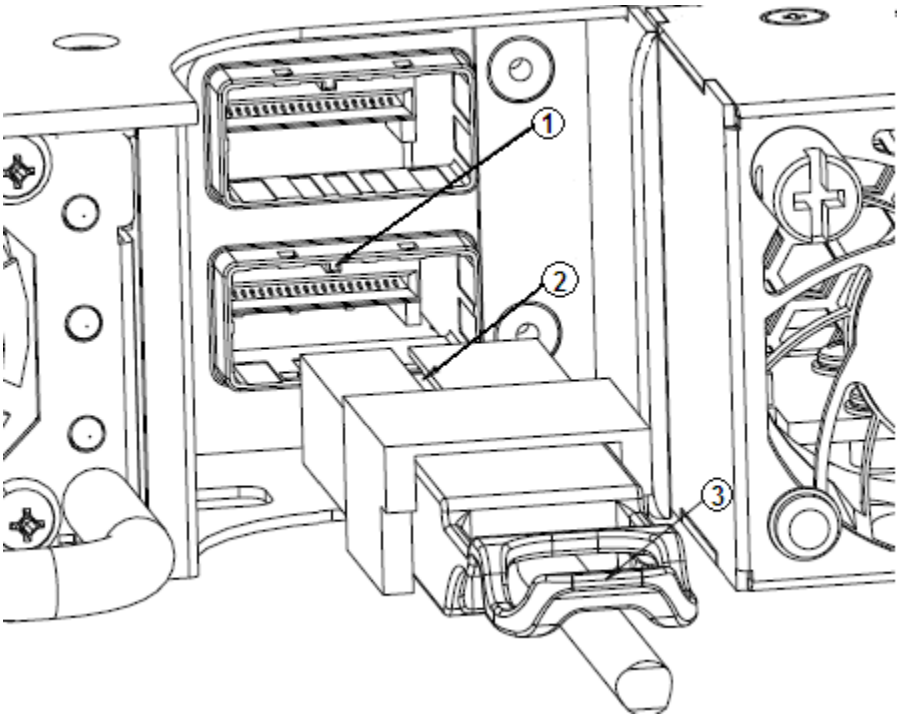


Figure 1: Installing Fabric Interconnect cables



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

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.

Caution:

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, Software Release 10.1, software files. File sizes are approximate.

Module or file type	Description	File name	File size (bytes)
Standard runtime image software version 10.1.	Agent software image for the Avaya Virtual Services Platform 7000 Series	7000_101000.img — non-secure image 7000_101001s.img — secure image	10,088,628 10,322,372
Diagnostics software version 10.1.	Diagnostics software for the Avaya Virtual Services Platform 7000 Series	7000_10106_diags.bin — diagnostics 10.1.0.6	3,866,700
MIB Definition Files for software version 10.1.	MIB Definition Files	Virtual_Services_Platform_70xx_MIBs_10.1.0..zip	1,142,221

Software and hardware capabilities

The following table lists supported software and hardware scaling capabilities for the Avaya Virtual Services Platform 7000 Series Software Release 10.1.

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

Feature	Maximum number supported
General	
MAC addresses	131,071
Egress queues	Configurable 1–8
Lossless mode queue set size	2
QoS precedence	1–10
QoS rules	Up to 15 policies per port Up to 63 meters per port Up to 125 filters per port Up to 256 filter components per precedence per device Up to 128 metes per precedence per device Up to 128 counters per precedence per device Up to 16 TCP/UDP port range checkers per device
Maximum number of Port Mirroring Instances	1
Fabric Interconnect bandwidth	5120 Gbps per Fabric Interconnect Stack (full duplex)
Maximum number of units in a virtual fabric (stack).	8
Layer 2	
Avaya Spanning Tree Groups	8
Multi-Link Trunking (MLT), Distributed Multi-Link Trunking (DMLT), and Link Aggregation (LAG) groups	32
MLT Links or ports per MLT, DMLT, or LAG	8
MLT Maximum MAC Learning rate on an MLT trunk	1300-1500 new MAC addresses per second

Feature	Maximum number supported
Spanning Tree Group instances (802.1s)	8
VLAN Concurrent VLANs	1024
VLAN Supported VLAN IDs	1–4094 • 0 and 1095 reserved • 4001 reserved by STP • 2004–2008 reserved by multiple STP groups
VLAN Protocol-based VLANs	7
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
Miscellaneous	
LLDP Neighbors per port	16
LLDP Neighbors	800
RMON alarms	800
RMON events	800
RMON Ethernet statistics	110
RMON Ethernet history	249
Telnet Client IPv6	4 sessions
Telnet Server IPv6	4 sessions
HTTP Server IPv4	3 sessions
HTTP Server IPv6	3 sessions

Supported browsers

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

- Microsoft Internet Explorer 8.0
- Mozilla Firefox 7.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

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. Log on to the ACLI Privileged Executive mode.
2. At the command prompt, enter the following command:

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

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*>	The IPv4 or IPv6 address of the TFTP server on which the agent image is hosted. • A.B.C.D — Specifies the IP address in IPv4 format. • WORD — Specifies the IP address in IPv6 format. The address parameter is optional and, if omitted, the switch defaults to the TFTP server specified by the **tftpserver** command unless software download is to take place using a USB mass storage device.
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.
<*usb*> | <*tftp*> | <*sftp*>	Specifies the software download source. • USB — download is from a USB mass storage device. • TFTP — download is from a TFTP server. • SFTP — download is from a SFTP server.

Variable	Value
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).

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.
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.

Variable	Value
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. • dnldFwFromUsb — Downloads the diagnostic image from a USB storage device.
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 802.1AB Layer Link Discovery 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 802.1w Rapid Spanning Tree Protocol
- IEEE 802.3 Ethernet
- IEEE 802.3u Fast Ethernet
- IEEE 802.3x Flow Control
- IEEE 802.3z Gigabit Ethernet
- IEEE 802.3ab Gigabit Ethernet over Copper
- IEEE 802.3ad Link Aggregation Control Protocol
- IEEE 802.3ae 10 Gbit/s Ethernet over fiber
- IEEE 802.3aq Ethernet over multimode fiber

RFCs and MIBs

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

- RFC 1769 SNTP
- 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 DHCP
- RFC 2138 RADIUS
- RFC 2236 IGMPv2
- RFC 2460 Internet Protocol Version 6
- RFC 2461 Neighbor Discovery for IPv6
- RFC 2462 Auto-Configuration for Link Local Addresses
- 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 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 4007 Scoped Address Architecture

- RFC 4022 TCP MIB
- RFC 4113 UDP MIB
- RFC 4293 IPv6
- RFC 4432 SSH RSA
- RFC 4443 ICMPv6

Chapter 3: Resolved issues

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

Resolved issues for Release 10.1

The following table lists the issues resolved in the current software release.

Reference number	Description
wi00885431	**Auto-negotiation**: The **`show auto-negotiation`** command now provides the correct output for SFP+ ports.
wi00905866	**Flow Control, SFP to SFP+**: If you have an SFP device plugged into a port which has an active link and then replace that with a SFP+ device, the port will now display the correct flow control mode.
wi00923626	**Interface Output**: The **`show interfaces verbose`** command now outputs the correct information.
wi00930397	**IP Management Address**: If you issue the **`renew dhcp`** command to refresh the switch IP address, the system will no longer display a number of ARP error messages.
wi00907504	**IP Management Address, MLT, STGs**: When the switch has learned a large number of MAC addresses (greater that 110,000) across multiple MLT links in different spanning tree groups, traffic to the management IP address will no longer be impacted.
wi00881570	**IPMGR**: When you use the **`show ipmgr`** command, the system now correctly displays IPv6 Information.
wi00925076	**MAC Address**: When you issue the **`show mac port x address y`** command, the system will now correctly display the MAC address for the port.
wi00908923	**MIBs**: The following MIB values are correctly updated: dot3StatsDuplexStatus,

Reference number	Description
	dot3StatsRateControlAbility, dot3StatsRateControlStatus
wi00896020	**MLT**: The **`show mlt hash-calc`** command now displays the correct output when no parameters are specified.
wi00904811	**Oversized Packet Counter**: The system now correctly increments the oversized packet counter.
wi00897460	**Password Aging, ASCII Configuration Reload**: If you enable password security on a switch, then copy the configuration to a TFTP server using the command **`copy running-config verbose`**, the system now writes the correct password aging command to the configuration file.
wi00921317	**Password History**: If you download a binary configuration to a switch, the password history is now correctly restored.
wi00900883	**Rate Limiting**: If you set rate limiting on a port to exactly 11 packets per second (pps), the system now configures rate limiting correctly.
wi00923803	**Show running-config module**: The CLI commands **`show running-config module stack`** or **`show running-config module mac-security`** now produce meaningful information as these features are present.
wi00881833	**SNMP Server**: When you use the **`show snmp-server host`** command the system now correctly displays IPv6 Information.
wi00884794 wi00885385 wi00891743 wi00891763 wi00891810 wi00891817 wi00892276 wi00924836	**USB**: The VSP 7000 now fully supports the USB port and USB devices to transfer files and images to and from the switch.
wi00923898	**USB issue**: An error is no longer displayed when downloading diag/bootloader from USB device.

Chapter 4: 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 10.1. Where available and appropriate, workarounds are provided.

Reference number	Description
wi00996632	**10m Fabric Interconnect**: When the 10m Fiber Fabric Interconnect cable (AL77018005–E6) is used with the VSP 7000 running release 10.1, packet errors might be seen on the connection if the ambient temperature is approaching 50 degrees Celsius. **Workaround**: When the switch is operating in lower ambient temperatures (for example, below 40C), the errors are not seen.
wi00995011	**7008XLS MDA, Resource Counters**: When the ports on the 7008XLS MDA are oversubscribed due to known Unicast traffic, the “Dropped on no resources” counter does not increment.
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.
wi00980557	**Broadcast, Multicast Rate Limiting**: When running the `show rate-limit` command, the multicast rate displayed for the past 24 hours might be incorrect.
wi00978314	**EDM, 32 ports**: When using Enterprise Device Manager (EDM) with the VSP 7000, some work areas might

Reference number	Description
	incorrectly indicated 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.
wi00978187	**EDM, Help Files**: When the Fabric Interconnect Stack is running from a Temporary Base Unit (TBU), then Enterprise Device Manager (EDM) is unable to access Help Files even if these were previously configured.
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.
wi00946937	**EDM, TACACS password**: If ACLI password type is set to TACACS, when you connect to the switch using Enterprise Device Manager (EDM), it does not prompt for a username or password.
wi00980352	**EDM, TCP Listeners**: When using Enterprise Device Manager (EDM), the switch does not display TCP Listeners for IPv4.
wi00952515	**EDM, VLAN range**: When using Enterprise Device Manager (EDM), it is not possible to specify a VLAN range when trying to add a new L2 Classifier Element. **Workaround**: Use ACLI to add the L2 Classifier Element when a full VLAN range is required.
wi00898211	**IP Management Address**: If you configure an IP address for the switch management which already exists on the network, the switch does not generate a duplicate IP address warning.
wi00947420	**IPv6 Management Address**: The switch does not auto-configure the IPv6 management address when receiving RouterAdvertisements with a valid prefix. **Workaround**: Manually configure the IPv6 management address.

Reference number	Description
wi00971757	**Lossless Mode**: When the switch is operating in Lossless mode and flowcontrol is disabled on a port, the dropped on no resources counter stays at zero on egress port, even if the port becomes over-subscribed. **Workaround**: You must enable flow control on all ports if the switch is operating in Lossless mode.
wi00997689	**Lossless Mode, Flow Control, SFP+**: When operating in Lossless mode and flow control is enabled on SFP+ ports, if the SFP+ device is unplugged, and then plugged back in, the port reverts to flow control disabled. **Workaround**: Once you re-insert an SFP+ device, you must re-enable flow control on the port if the switch is operating in Lossless mode.
wi00996142	**Lossless Mode, RSTP**: When operating in Lossless mode with RSTP enabled, in some situations of network recovery, pause frames can be looped within the network leading to traffic being incorrectly paused. **Workaround**: Avaya recommends to not enable RSTP if the switch is operating in Lossless mode.
wi00882399	**MAC Addresses**: In some situations, the VSP 7000 does not learn all 131,072 MAC Addresses.
wi00960906	**MLT**: If running 100% line rate traffic on all MLT links, the `show mlt utilization` command might incorrectly display an MLT utilization of approximately 92% for each MLT link.
wi00973130	**MSTP**: When a Fabric Interconnect Stack is configured with MSTP mode of operation and a large number of VLANs, redundant MLT links are present, resting a non Base Unit could result in a broadcast storm if the network contains many redundant loops. **Workaround**: If after rebooting a non Base Unit in a complex network results in a broadcast storm, it has been found that bouncing the interfaces on the offending unit typically stops the broadcast storm.
wi00959872	**Port Mirroring, XrxYtx Mode**: Multicast and unknown Unicast frames are not mirrored when XrxYtx port mirroring mode is used.
wi00928140	**Quality of Service, Equal Drop Precedence**: When egress traffic is oversubscribed, packets of equal size with the same high drop precedence might not experience equal drop distribution. **Workaround**: Introducing traffic of different packet sizes or drop precedence will result in expected results.

Reference number	Description
wi00968076	**Quickconfig, IPv6 delay**: When running quickconfig script, occasionally the script might pause for up to 10 seconds after entering an in-band IPv6 address.
wi00973969	**RADIUS, Telnet Disconnect, Accounting Messages**: When a telnet session to the switch is closed and RADIUS accounting is enabled, the switch will incorrectly generate two radius messages. One with the Acct-Status-Type attribute set to “User Request” and one with attribute set to “Lost Carrier”.
wi00940709	**RMON, ACLI**: Display of RMON event Community and LastTimeSent information is not available when using ACLI. **Workaround**: Use EDM to display the required information.
wi00929094	**Stack Loopback test (External)**: The External Stack Loopback can only be performed between the TOP FI-ports. Testing an FI cable with the BOTTOM FI-ports can result in a false pass. The cable contains three 40Gb channels, but only one channel is available on the bottom FI-ports. **Workaround**: You must test all FI cables using the TOP<->TOP FI-ports only.
wi00994847	**Stack Loopback test (Internal)**: When performing an internal Fabric Interconnect Stack loopback test, a failure message is always displayed. **Workaround**: Avaya recommends to not perform Stack Loopback tests in Release 10.1.
wi00934503	**Traceroute**: If you have two VSP 7000 switches directly connected to each other, performing a traceroute from one switch to the other will fail; even though the switches can be reached using the ping command.
wi00984580	**USB**: When using older USB devices, on first insertion the USB device might not be initially recognized by the VSP 7000. **Workaround**: Remove and reinsert the USB device, in most cases the device is correctly detected.
wi00974439	**USB**: Saving the binary config might fail when saving to a USB device which is not connected to the Base Unit (BU) or Temporary Base Unit (TBU) of a Fabric Interconnect Stack with a large number of units. **Workaround**: It is recommended to use a USB device connected to the Base Unit (BU) or Temporary Base Unit (TBU). If you are using a USB device in another unit to perform a binary configuration save and an error occurs, then repeating the operation typically results in a successful save of the binary config to USB.

Reference number	Description
wi00974728	**VLACP, Traps**: Inconsistent logging of VLACP traps can occur if enabled.