Release Notes for Avaya Ethernet Routing Switch 5000 Series

Release 6.6.1
NN47200-400
Issue 10.01
July 2014

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

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

Licence types

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

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link “Heritage Nortel Products”, or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants 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 describes new features and important information about the latest release. Release notes include a list of known issues (including workarounds where appropriate) and a list of resolved issues. This document also describes known limitations and expected behaviors that may first appear to be issues.

This document describes new features, hardware, upgrade alerts, known and resolved issues, and limitations for the Avaya Ethernet Routing Switch 5000 Series, Release 6.6 and higher.

These release notes provide the latest information about the current software release, as well as operational issues not included in the documentation.

The information in this document supersedes applicable information in other documents in the suite.

Related resources

Documentation

See the *Documentation Reference for Avaya Ethernet Routing Switch 5000 Series*, NN47200–103 for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com.

Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com, 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.

Supported Switch Models

The Avaya Ethernet Routing Switch 5600 Series, supported by software release 6.6, includes the following switch models:

- Avaya Ethernet Routing Switch 5698TFD
- Avaya Ethernet Routing Switch 5698TFD-PWR
- Avaya Ethernet Routing Switch 5650TD
- Avaya Ethernet Routing Switch 5650TD-PWR
- Avaya Ethernet Routing Switch 5632FD

Configurations can vary from a stand-alone switch to a stack of up to 8 switches. A stack can consist of any combination of switches, with the restriction that the maximum number of ports supported in a stack is 400 ports. One of the benefits of operating Avaya Ethernet Routing Switch

5600 Series switches in a stack is management efficiency; a stack is managed with a single IP address and software is available as a single image across all models.

Note:

Release 6.6 supports pure stacks of 56xx switches only. Hybrid or mixed stacking of 55xx with 56xx switches and pure stacks of 55xx switches are not supported.

Chapter 2: New in this release

The following sections detail what's new in *Release Notes for Avaya Ethernet Routing Switch 5000 Series*, NN47200-400 for Release 6.6 and Feature Pack Release 6.6.1.

Features in release 6.6.1

See the following sections for information about feature changes in release 6.6.1.

Fabric Attach

Feature Pack Release 6.6.1 introduces Fabric Attach to ERS 5000 Series switches. Fabric Attach can extend the fabric edge to devices that do not support SPBM, so that these devices can take advantage of full SPBM support, if support is available.

ERS 5000 Series Fabric Attach support is limited to the Fabric Attach proxy function. Fabric Attach server and client operations are not supported.

For more information, see Fabric Attach on page 58.

IPFIX Export VLAN ID

IPFIX Export VLAN ID adds a new field to the registered flows, which are displayed in the IPFIX table for the observation ports, VLAN field.

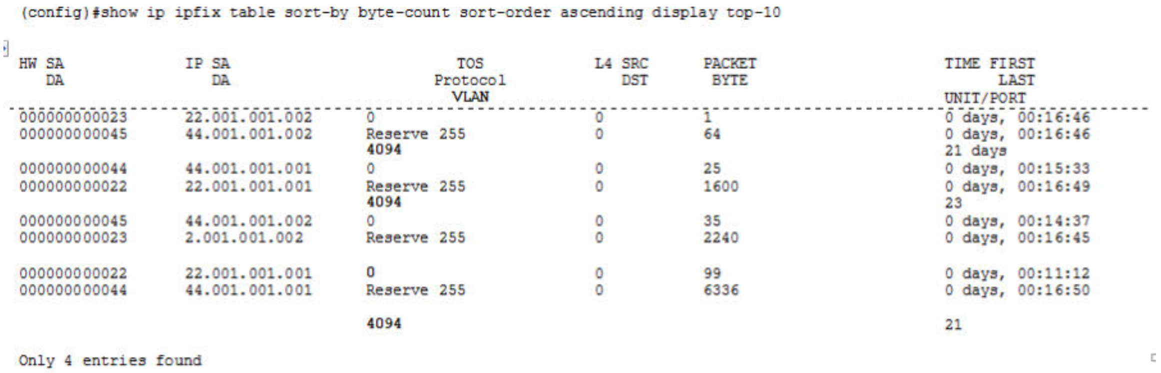
When the IPFIX exporter is enabled and a collector is configured for registered flows, the templates received at the collector should have the VLAN ID option present with all the VLAN IDs configured.

The double tagged traffic is seen by ASIC as L2 traffic. Because double tagged traffic is not captured and unpacked by ASIC, the IPFIX cannot display flows double tagged.

This feature is configured globally and on a port level.

The VLAN ID information for IPFIX can be seen with the following ACLI command.

The commands or parameters emphasized using bold typeface below are new, as shown in the following example.



```
(config)#show ip ipfix table sort-by byte-count sort-order ascending display top-10

HW SA            IP SA                    TOS          L4 SRC    PACKET                      TIME FIRST
   DA               DA                  Protocol          DST     BYTE                               LAST
                                          VLAN                                               UNIT/PORT
-------------------------------------------------------------------------------------------------------------
000000000023     22.001.001.002     0                   0        1                           0 days,  00:16:46
000000000045     44.001.001.002     Reserve 255         0        64                          0 days,  00:16:46
                                    4094                                                     21 days
000000000044     44.001.001.001     0                   0        25                          0 days,  00:15:33
000000000022     22.001.001.001     Reserve 255         0        1600                        0 days,  00:16:49
                                    4094                                                     23
000000000045     44.001.001.002     0                   0        35                          0 days,  00:14:37
000000000023     2.001.001.002      Reserve 255         0        2240                        0 days,  00:16:45

000000000022     22.001.001.001     0                   0        99                          0 days,  00:11:12
000000000044     44.001.001.001     Reserve 255         0        6336                        0 days,  00:16:50

                                    4094                                                     21

Only 4 entries found
```

There is no EDM support for this VLAN ID information for IPFIX.

Lockout for failed logon attempts

The lockout for failed logon attempts feature prevents brute force hacking. Following a consecutive number of log on failures, all password logon interfaces (telnet, SSH and web) are disabled for a configurable amount of time. The default lockout interval is one minute.

Features in release 6.6

See the following sections for information about feature changes in release 6.6.

802.1X-2004 support

With the 802.1x-2004 standard the switch can authenticate both EAPOL version 1 and EAPOL version 2 supplicants.

For more information on EAPOL, see:

- *Configuring Security on Avaya Ethernet Routing Switch 5000 Series*, NN47200-501

802.1X: Default all EAP settings

This feature allows you to default all EAP settings globally and on a port level.

For more information, see:

- *Configuring Security on Avaya Ethernet Routing Switch 5000 Series*, NN47200-501

802.1X: Fail Open VLAN Continuity mode

The Fail Open VLAN Continuity mode feature introduces a new mode of operation for EAP/NEAP clients when the RADIUS server(s) become unreachable.

For more information, see:

- *Configuring Security on Avaya Ethernet Routing Switch 5000 Series*, NN47200-501

802.1X: Maximum number of EAP and NEAP clients per port

You can define the maximum number of EAP and Non-EAP clients allowed per port, from one client up to 64, where 64 would be a maximum of 32 EAP clients and 32 NEAP clients. The default for the maximum number of clients is one. There is no priority of EAP or NEAP clients for authentication.

To configure the maximum clients parameter, see:

- *Configuring Security on Avaya Ethernet Routing Switch 5000 Series*, NN47200-501

802.1X: NEAP not member of VLAN

The NEAP not member of VLAN feature ensures that ports configured with RADIUS Non-EAP authentication are assigned to at least one VLAN to make authentication possible for Non-EAP clients.

For more information, see:

- *Configuring Security on Avaya Ethernet Routing Switch 5000 Series*, NN47200-501

802.1X: NEAP Phone (Avaya Support)

NEAP IP Phone support is enhanced to recognize Avaya Red handsets through two additional DHCP signatures: Nortel-SIP-Phone-A and ccp.avaya.com.

802.1X: NEAP support for freeform password

The ability to support complex passwords for NEAP switch authentication is extended with the use of a global freeform password. A CLI configurable key consisting of a string of up to 32 ASCII characters is added to the NEAP password format used to authenticate NEAP clients.

For more information, see:

- *Configuring Security on Avaya Ethernet Routing Switch 5000 Series*, NN47200-501

ACLI show flash history command

The `show flash history` command provides the current status of the Flash device. You can use the `show flash history` command to view the flash writes and erase history on a standalone unit or stack. The Flash History does not record programming done 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 get corrupted during an upgrade or downgrade. Flash History is automatically enabled and does not require any configuration.

For more information on the `show flash history` command, see:

- *Getting Started with Avaya Ethernet Routing Switch 5000 Series*, NN47200–303

.

ARP scaling

In Release 6.6, the total number of ARP table entries is increased to 4,096.

For more information on ARP, see:

- *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5000 Series*, NN47200-503

Change RADIUS Password

If you have RADIUS servers in your network, you can allow users to change account passwords when they expire.

Note:

Change RADIUS password is available only in secure software builds.

You can enable or disable the Change RADIUS password feature. By default, this feature is disabled. When Change RADIUS password feature is enabled, the server reports the password expiry and system prompts you to create a new password.

For more information about the Change RADIUS password feature, see:

- *Configuring Security on Avaya Ethernet Routing Switch 5000 Series*, NN47200-501

CLI list command

This feature provides an enhancement to the CLI `help` command, by adding a complete list of the CLI tree available on the unit, regardless of the current unit configuration. You can also use the “verbose” option to list the syntax of every CLI command.

For more information, see:

- *Fundamentals of Avaya Ethernet Routing Switch 5000 Series*, NN47202-104

Default IP

The Ethernet Routing Switch 5600 Series sets an IP address of 192.168.1.1/24 by default if the switch does not obtain its IP from another source.

Note:

As this feature overrides the UI button functionality to set the default IP address, the UI button functionality has been removed.

For more information, see:

- *Getting Started with Avaya Ethernet Routing Switch 5000 Series*, NN47200–303

EDM improved download support

When downloading software to the switch, EDM provides a status bar on the progress and an indication when the download is complete.

For more information, see:

- *Getting Started with Avaya Ethernet Routing Switch 5000 Series*, NN47200–303

EDM inactivity timeout

You can configure the period of time that an EDM session remains idle before the session expires. The current default expiry for an idle EDM session is 15 minutes.

For more information, see:

- *Getting Started with Avaya Ethernet Routing Switch 5000 Series*, NN47200–303

Link-state tracking

The link-state tracking feature binds the link state of multiple interfaces, so that if a specified interface or its Virtual Link Aggregation Control Protocol (VLACP) state goes down, all the other interfaces in that group are placed in a temporary down state.

For more information, see:

- *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5000 Series*, NN47200–502

Out-of-band management

Out-of-band management allows switch or stack management through the dedicated out-of-band management port. This port can accept an IPv4 or IPv6 address different from the switch or stack IP address. With out-of-band management, you do not require an in-band management VLAN to carry switch or stack management traffic, including Telnet, Secure Shell (SSH) protocol, Simple Network Management Protocol (SNMP), HTTP, or HTTPS. You can also use out-of-band management to download a software image or access the Enterprise Device Manager (EDM) interface for a switch or stack.

For more information, see:

- *Getting Started with Avaya Ethernet Routing Switch 5000 Series*, NN47200–303

Remote Switch Port Analyzer (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 on the network.

For more information, see:

- *Configuring System Monitoring on Avaya Ethernet Routing Switch 5000 Series*, NN47200-505

RO User access to Telnet and SSH

Users logged in with read-only permission can now have access to Telnet and SSH commands. Previous software releases required the user to be logged in with read-write access.

For more information on using Telnet and SSH, see:

- *Configuring Security on Avaya Ethernet Routing Switch 5000 Series*, NN47200-501

Run Scripts

You can use the run scripts to automatically configure the parameters for an Avaya Stackable Ethernet switch according to Avaya's best practices for converged solutions. The scripts can be executed in a default or verbose mode.

In the default mode, the switch is configured using predetermined parameter values. In the verbose mode, you can modify the default values and settings when the script is executed.

In this release, run scripts are available for IP Office, Link Layer Discovery Protocol (LLDP), and Auto Detect Auto Configuration (ADAC).

For more information, see:

- *Getting Started with Avaya Ethernet Routing Switch 5000 Series*, NN47200–303

Secure File Transfer Protocol (SFTP) enhancements

For secure (SSH) software images, the SFTP client functionality is enhanced to include download support of agent and diagnostic files, ASCII configuration file download and upload, download of license files, and DHCP external save transfer to and from an SFTP server.

For more information, see:

- *Configuring Security on Avaya Ethernet Routing Switch 5000 Series*, NN47200-501

Show TCP Ports

You can view information about active IPv4 sockets similar to the output from the Unix netstat command.

For more information, see:

- *Configuring System Monitoring on Avaya Ethernet Routing Switch 5000 Series*, NN47200-505

Show UTC timestamp

The show UTC timestamp feature enables you to display the UTC timestamp after issuing any show command in ACLI. By default, the timestamp state is disabled.

For more information, see:

- *Getting Started with Avaya Ethernet Routing Switch 5000 Series*, NN47200–303

SLA Monitor

The Service Level Agreement (SLA) Monitor is an embedded monitoring device designed to identify and isolate performance issues in a network.

For more information, see:

- *Configuring System Monitoring on Avaya Ethernet Routing Switch 5000 Series*, NN47200-505

SSH Client

SSH Client is a secure shell protocol for connecting to an SSH server accepting remote connections, and is a secure alternative to telnet. The SSH Client uses SSH version 2 and is present only on secure (SSH) images.

For more information, see:

- *Configuring Security on Avaya Ethernet Routing Switch 5000 Series*, NN47200-501

VRF ping support

The ping command allows you to specify the VRF.

For more information, see:

- *Getting Started with Avaya Ethernet Routing Switch 5000 Series*, NN47200–303

VRF stacking and traceroute support

In Release 6.6, VRF is now available for stacked 5600 configurations. In addition, you can specify the VRF in the traceroute command.

For more information on VRF, see:

- *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5000 Series*, NN47200-503

Other changes

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

CLI interface change from FastEthernet to Ethernet

The CLI interface command `interface FastEthernet` is changed to `interface Ethernet`. The FastEthernet interface command remains available, but hidden so as to provide backward compatibility.

Removal of DAUR support

DAUR support has been removed for Avaya ERS 5600 Series in Release 6.6.

Removal of hybrid stack support

Release 6.6.1 supports 5600 and pure stack of 5600 only. ERS 5500 in stack (pure/hybrid) or standalone is not supported.

Removal of NSNA support

NSNA support has been removed for Avaya ERS 5600 Series starting in Release 6.6.

Removal of QoS filter limiting

Since Release 6.6 is not supported on ERS 5510 units that require QoS filter limiting, Release 6.6 removes ACLI commands and EDM support for QoS filter limiting.

Chapter 3: Important notices and new features

This section describes important software and hardware related notices in the Avaya Ethernet Routing Switch 5000 Series Release 6.6.

Feature document location

The following table contains a list of key software features and their location in the documentation suite.

Table 1: Where to find information about key software features

Feature	Document
QoS Traffic Profiling Support	*Configuring Quality of Service on Avaya Ethernet Routing Switch 5000 Series*, NN47200-504
SMLT configuration	*Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5000 Series*, NN47200–502

Release file names

The following table describes the Avaya Ethernet Routing Switch 5600 Series software components for this release.

Table 2: Release 6.6.1 software components

File Type	Description	File Name	File Size (bytes)
Standard runtime image software version 6.6.1	Standard non SSH image for the Ethernet Routing Switches 5600 Series	5xxx_661032.img	10,762,932
Secure runtime image software version 6.6.1	Standard SSH image for the Ethernet Routing Switches 5600 Series	5xxx_661033s.img	11,025,540

File Type	Description	File Name	File Size (bytes)
Diagnostic software version 6.0.0.18	ERS5600 diagnostic software	5xxx_60018_diags.bin	2,471,456
Enterprise Device Manager Help Files	EDM Help files zip	ERS5000v660_HELP_EDM.zip	2,558,376
MIB Definition File	MIB Definition File	Ethernet_Routing_Switch_5xxx_MIBs_6.6.1.zip	1,621,217
COM Plug in	ERS5600 plugin for COM	ers5000v6.6.1.0.zip	3,841,225

Software upgrade

The procedures in this section are used to upgrade the diagnostic and agent software. Use these procedures to upgrade to Software Release 6.6 and higher.

❗ **Important:**

There is no upgrade path from any agent software release earlier than 6.3 to Software Release 6.6. Devices running older agent software must first be upgraded to a version of Software Release 6.3 before upgrading to Software Release 6.6. Note that the diagnostic software running on the device should not be earlier than 6.0.0.16.

❗ **Important:**

If upgrading from a 5.x diagnostic image to a 6.x diagnostic, you should not use the no-reset option. You must execute the 6.x diagnostic prior to loading any 6.x agent images.

Upgrading diagnostic software

Use the following procedure for upgrading the diagnostic software image.

1. Access the ACLI through a Telnet or Console connection.
2. Enter Privileged EXEC mode using the **`enable`** command.
3. Use the command **`download address <ip_address> diag <image_name> [no-reset] [usb]`** to transfer the diagnostic image to the device.

The following table describes the parameters for the download diag command.

Parameter	Description
address <ip_address>	The IPv4 or IPv6 address of the TFTP server on which the diagnostic image is hosted.
diag <image_name>	The name of the diagnostic image file on the TFTP server.
no-reset	This parameter specifies that the device will not reset after the upgrade is complete.

Parameter	Description
usb	This parameter specifies that the software download will occur from a USB device instead of the network.

The upgrade process occurs automatically without user intervention. This process deletes the contents of the flash memory and replaces it with the desired software image. Do not interrupt the download process.

When the process is complete, the device automatically resets unless the **`no-reset`** parameter was used. The software image initiates a self-test and returns a message when the process is complete.

During the download process the switch is not operational.

Upgrading agent software

Use this procedure to upgrade agent software.

1. Access the ACLI through a Telnet or Console connection.
2. Enter Privileged EXEC mode using the **`enable`** command.
3. Use the command **`download address <ip_address> {primary | secondary} {image <image_name> | image-if-newer <image_name> | poe_module_image <image_name>} [no-reset] [usb]`** to transfer the agent image to the device.

The following table describes the parameters for this command.

Parameter	Description
address <ip_address>	The IPv4 or IPv6 address of the TFTP server on which the agent image is hosted.
primary | secondary	Designates whether the image is stored in the primary or secondary image location. The default is primary.
image <image_name> | image-if-newer <image_name> | poe_module_image <image_name>	The name of the agent image file on the TFTP server. Each option is mutually exclusive. Use the option described with the following situation: • To load the agent image under normal circumstances, use the image option. • To load the agent image only if it is newer than the current image, use the image-if-newer option. • To load the agent image if it is a PoE module image, use the poe_module_image option.
no-reset	Specifies that the device will not reset after the upgrade is complete.
usb	Specifies that the software download will occur from a USB device instead of the network.

The upgrade process occurs automatically without user intervention. This process deletes the contents of the flash memory and replaces it with the desired software image. Do not interrupt the download process.

When the process is complete, the device automatically resets unless the `no-reset` parameter was used. The software image initiates a self-test and returns a message when the process is complete.

During the download process the switch is not operational.

Upgrade strategy if DHCP snooping, DHCP relay or NonEap Phone Authentication use DHCP signature

Use the following upgrade strategy if the DHCP snooping or NonEap Phone Authentication uses DHCP signature or DHCP relay in the network.

Upgrade strategy	Upgrade all switches in your network if the switches are running software versions prior to the versions mentioned in the following: • ERS 25xx: 4.4.3. ✱ **Note:** Note: ERS 25xx is in End of Sales and currently there is no schedule planned for 4.4.3 software version. • ERS 35xx: 5.1.2, 5.2.x • ERS 4xxx: 5.6.4, 5.7.1, 5.8.x • ERS 5xxx: 6.2.8, 6.3.3, 6.6.x • VSP 7xxx: 10.3.2, 10.4.x ✱ **Note:** Upgrade the affected ERS switches closest to the client devices first and then progress towards the core.
Issue	In some previous software releases of the Stackable ERS platforms (ERS 2500, 3500, 4000 and 5000 Series) as well as the VSP 7000, a software issue was found to cause malformed DHCP packets as they were forwarded out of the switch. In the software releases listed in the preceding row, a code change has been made to stop the malformed packets from being generated and also to discard these malformed packets if the switch is receiving them.

	Due to the nature of the code change, there are potential interaction scenarios between ERS switches running different code versions which will need to be managed within the context of a network upgrade to releases containing the code changes.
Implications if this upgrade strategy is not followed	DHCP packets which previously transitioned the network without issue may now be lost if using ERS switches which utilize mixed agent versions with and without this fix.
Workaround if this upgrade strategy is not followed	• Disable the DHCP features (DHCP snooping, DHCP relay or DHCP signature authentication) on switches running the older software versions so that the malformed DHCP packets are not generated. Implementation of this option is dependent on the network topology that still allows DHCP packets to reach the DHCP server and may require additional configuration changes. • Disabling DHCP snooping or DHCP relay on switches running the software with the fix will prevent malformed DHCP packets from being dropped if they are received from other switches that are not upgraded. Implementation of this option may also require additional configuration changes to ensure that the DHCP requests reach the DHCP server.

For more information, see https://kb.avaya.com/kb/index?page=content&id=SOLN251146

How to get EDM online help files for embedded EDM

Because help files are not included with the embedded EDM software files on the switch, a network administrator must copy the software-release-specific help files onto a TFTP server. Once the help files are downloaded to the TFTP server, the network administrator must configure the switch with the path to the help files on the TFTP server. You can use ACLI or EDM to configure a path from your switch to the help files. After the path to the help files is configured, whenever an EDM user clicks the help button on the toolbar, the switch downloads and displays help information in the Web browser.

If you are using Configuration and Orchestration Manager (COM) to manage your switch, help resides with COM and you do not need to use these procedures.

For more information about EDM, see *Fundamentals of Avaya Ethernet Routing Switch 5000 Series*, NN47202-104.

Downloading help files

Before you begin

- An available TFTP server

About this task

Use this procedure to download EDM online help files.

Procedure

1. To obtain EDM help files for the embedded element manager, do one of the following:
   - Go to the Avaya Web site at http://www.avaya.com/support and locate the help files for the appropriate product.
   - Select the help files from the software CD ROM.
2. Download the help files to a TFTP server.

How to configure the path to the embedded EDM help files

If you are using embedded EDM, use the procedures in this section to configure the path to the help files. You can configure the help file path with ACLI or EDM.

Configuring the path to the help files using ACLI

About this task

Use the following procedure to configure the path to the help files using ACLI.

Procedure

In ACLI, go to the Global Configuration mode and use the following command:

```
edm-help-file-path <path name> tftp address <tftp address>
```

The following table describes the parameters for the edm-help-file-path command.

Parameter	Description
path name	Specifies the path name you created for EDM help files. The path name is stored in NVRAM.
TFTP address	Specifies EDM TFTP server IP address. Use this address only for EDM help files. If you do not specify a TFTP server address, the system uses the address specified most recently.

Parameter	Description
	WARNING: Because the TFTP server address is stored in NVRAM, each time the system returns to the default configuration, you must reconfigure the path to EDM online help.

Example

Following is an example of an ACLI EDM help file path:

```
edm help-file-path ERS5000_66_Help tftp address 100.100.100.15
```

In the preceding example ERS5000_66_Help is a folder that contains help files and the folder is located on a TFTP server at the 100.100.100.15 address.

Configuring the path to the help files using EDM

Use the following procedure to configure the path to the help files.

Procedure steps

1. From the navigation tree, click **Edit**.
2. From the Edit tree, click **File System**.
3. Select the **Help File Path** tab.
4. In the Path dialog box, enter the path to the help file storage location.

   Example

   tftp://xxx.xxx.xxx.xxx/file_name

Supported software and hardware capabilities

The following table lists the known limits for the Avaya Ethernet Routing Switch 5000 Series, Release 6.6 and higher, and Enterprise Device Manager.

Table 3: Supported software and hardware capabilities

Feature	Maximum number supported
VLANs	1024 (1k)
Protocol-based VLANs	Depending on the protocol specified, the number of protocol VLANs supported at one time varies between 3–7. See *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5000 Series*, NN47200–502 for more information.
IGMP maximum number of unique groups	Layer 2 and Layer 3

Feature	Maximum number supported
	992
EAPoL 802.1x supplicants	32 per port 768 per stack
Maximum number of routes (dynamic, static and local)	4000 routes for ERS 5600 units and stacks
ARP records	4096
Static ARP	256
IP interfaces	256
Static routes	512
Spanning Tree Groups	8
IPv6 DHCP relay forward paths	256
IPv6 static routes	512
IPv6 interfaces	256
IPv6 tunnels	4
Aggregation groups (link aggregation)	32
Ports per aggregation group	8
MAC addresses in fdb	16 K
OSPF areas	4 (3 areas plus area 0)
OSPF adjacencies	64
VRRP interfaces	64
ECMP	4 paths
DHCP Snooping Binding table entries	1024 per switch
DHCP relay forward paths	512
IP Management routes	4
PIM-SM multicast entries	Up to 992 for ERS 56xx series The ERS 56xx platforms support a maximum of 992 IPMC forwarding entries. These limitations are imposed on standalone ERS 56xx devices and stacks. Note: These limits do not indicate that 992 entries will actually be available since the installation of IPMC entries in hardware is also determined by free entries being available.
Allow-flood IGMP multicast addresses	The maximum number of allow-flood multicast entries is determined by the number of VLANs on the device. Each entry in the allow-flood table applies to each current VLAN; for example, if 1 entry exists in the allow-flood table and 5 VLANs are configured, then there are 5 entries programmed in hardware.

Feature	Maximum number supported
	Currently, the hardware limit is 4096. Note: You should not exceed this limit. The limit for the maximum number of allow-flood addresses is 128 (1 VLAN).
Link State Tracking: Instances	2
Port Mirroring: Instances	4
Port Mirroring: RSPAN VLANs	4
Port Mirroring: RSPAN destinations	4 per switch or stack
VRF: Instances	4
Neap supplicants	32 per port 768 per stack

Additional information for the software feature license file

When you create a license file to enable licensed features on an Avaya Ethernet Routing Switch 5000 Series switch with the Avaya Electronic Licensing Portal, you must specify a file name. Follow the instructions on the License Certificate within the License Kit, or for more information, see *Fundamentals of Avaya Ethernet Routing Switch 5000 Series*, NN47202-104.

You must use the following rules when you generate and name the file:

- A maximum of 63 alphanumeric characters
- Lower case only
- No spaces or special characters allowed
- Underscore (_) is allowed
- The dot (.) and three-character file extension are required

File name example, abcdefghijk_1234567890.lic.

The format of the file that you upload to the license generation tool, and that contains the list of MAC addresses, must be as follows:

- ASCII file format
- One MAC address per line
- No other characters, spaces, or special characters allowed
- MAC must be in hexadecimal, capitalized format, with each pair of characters separated by colon; for example, XX:XX:XX:XX:XX:XX
- The file must contain the correct MAC addresses. Any incorrect MAC addresses will result in the licensed features not working on designated units.

- The number of MAC addresses must not exceed the number of MAC addresses allowed for the License Authorization Code entered for a particular file. For example:
  - AL1016001 = 2 MAC addresses (1 stack/standalone unit)
  - AL1016002 = 20 MAC addresses (10 stacks/standalone units)
  - AL1016003 = 100 MAC addresses (50 stacks/standalone units)
  - AL1016004 = 200 MAC addresses (100 stacks/standalone units)

Supported standards, MIBs, and RFCs

This section lists the standards, MIBs, and RFCs supported by the Avaya Ethernet Routing Switch 5000 Series.

Standards

The following IEEE Standards contain information that applies to the Avaya Ethernet Routing Switch 5000 Series:

- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1X (EAPOL)
- IEEE 802.1ab (Link Layer Discovery 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)

RFCs

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

- RFC 768 (UDP)
- RFC 791 (IP)

- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 826 (ARP)
- RFC 854 (Telnet)
- RFC 894 (IP over Ethernet)
- RFC 951 (BootP)
- RFC 1112 (IGMPv1)
- RFC 1157 (SNMP)
- RFC 1213 (MIB-II)
- RFC 1271 (RMON)
- RFC 1350 (TFTP)
- RFC 1493 (Bridge MIB)
- RFC 1757 (RMON)
- RFC 1945 (HTTP v1.0)
- RFC 2131 (DHCP)
- RFC 2236 (IGMPv2)
- RFC 2362 (PIM-SM)
- RFC 2474 (QoS)
- RFC 2597 (QoS)
- RFC 2598 (QoS)
- 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 3140 (QoS)
- RFC 3246 (QoS)
- RFC 3376 (IGMPv3)
- 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 3576 (Dynamic Authorization Extensions to Remote Authentication Dial In User Service)

The following table lists IPv6 specific RFCs.

Standard	Description	Compliance
RFC 1886	DNS Extensions to support IPv6	Supported
RFC 1981	Path MTU Discovery for IPv6	Supported
RFC 2460	Internet Protocol v6 (IPv6) Specification	Supported
RFC 2461	Neighbor Discovery for IPv6	Supported
RFC 2462	IPv6 Stateless Address Auto-configuration	Auto-configuration of link local addresses only
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks	Supported
RFC 3162	RADIUS and IPv6	Supported
RFC 3315	DHCPv6	Support for IPv6 DHCP Relay
RFC 4007	Scoped Address Architecture	Supported
RFC 4022	Management Information Base for TCP	Mostly supported
RFC 4113	Management Information Base for UDP	Mostly supported
RFC 4193	Unique Local IPv6 Unicast Addresses	Not supported
RFC 4213	Transition Mechanisms for IPv6 Hosts and Routers	Supports dual stack and configured tunnels
RFC 4291	IPv6 Addressing Architecture	Support earlier version of RFC (3513)
RFC 4293	Management Information Base for IP	Mostly supported
RFC 4301	Security Architecture for the Internet Protocol	Not supported
RFC 4443	Internet Control Message Protocol (ICMPv6)	Support earlier version of RFC (2463)

Chapter 4: Resolved issues

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

Change Request Number	Description
Resolved issues in Release 6.6.1	
wi01120589	Pluggable Ports, EDM off-box - Pluggable Ports information cannot be obtained using the Pluggable Ports button from the EDM off-box. The button works only for EDM on-box.
wi01138674, wi01140590	DHCP Snooping external save - defaulting the DHCP Snooping external save settings results in wrong ACG output. Workaround: instead of defaulting the DHCP Snooping external save configuration prior to applying a new DHCP Snooping external save configuration, you can directly overwrite your settings.
wi01142391	Copper SFP - removing and reinserting a copper SFP may cause the switch to lose 10/00 port speed setting. Connectivity may be lost until the port speed is reset manually.
wi01105902	If an advice successfully EAP authenticated and at the same time its MAC is also MAC-based authenticated, the switch sees the device as two separate authenticated clients.
Resolved issues in Release 6.6	
wi00486525	VRRP may intermittently bounce when multiple protocols are configured on upstream routers with traffic and large routing updates.
wi00486579	Inconsistent display of pluggable modules in BigWave Stacks.
wi00486751, wi00490844, wi00497003	When the maximum of 10 DHCP clients are bound by IP Source Guard on MLT/LACP ports, if those ports go down, several IPSG binding table full messages will be logged. This is an incorrect behavior.
wi00487998	**Demo License**: If you use a Demo License and you remove the Demo License, you must reboot the stack.
wi00488227	EDM, Multiple Port Selection: EDM can delete up to a maximum of 120 ports when you use multiple port selection. If you select more than 120 ports, some of the ports may not disabled.
wi00488679	EDM: You cannot view and configure 802.1ab Dot1 settings for Local Protocol Vlan and Local Vlan Name using EDM. **Workaround**: Use ACLI to view and configure 802.1ab Dot1 settings for Local Protocol VLAN and Local VLAN name
wi00494658	A non-PoE phone may display as Unknown and need to be rebooted after a stack is rebooted.

Change Request Number	Description
Resolved issues in Release 6.6.1	
wi00554963	RADIUS, RADIUS reachability: If you use the "radius reachability use-radius", the switch sends reachability requests with the username 'avaya' and a blank password. Because the Avaya ignition server does not allow accounts to be created with a blank password, the ignition server will log intrusion events when the dummy requests are regularly sent from the switch. **WORKAROUND**: Use ICMP reachability for ignition server reachability.
wi00555156	SLPP: In a stack of 5 or more units that runs a complex configuration, for example, SMLT, LACP, SLPP, or OSPF, SLPP can fail to detect and prevent loops due to inadequate system resources. SLPP PDUs are not treated as high priority packets and are not processed on time. This does not happen on SLPP ports on the base unit.
wi00555215	EDM, MSTP: If your environment contains a large number of stacks and a large number of ports and you click between the CIST Port, MSTI Bridges, and MSTI Port tabs, the system may display the Unresponsive script dialog because you have initiated a large data retrieval.
wi00834482	When LACP and SLT's are configured IST's, some SLT ports may blocked traffic. If this happens, bouncing the SLT ports on the IST peers where the block occurs should resolve the issue and traffic can be seen forwarding again. This issue will address in the maintenance build.
wi00929935	Change in ADAC tagged frames configuration: You must delete LLDP MED network policies on phone and uplink/call server ports before configuring ADAC. There are default LLDP MED network policies on all ports that take precedence over ADAC policies.
wi00936876	OSPF, SMLT: An intermittent error may be seen when OSPF over SMLT is configured in a looped environment (SLPP enabled).
wi00982958, wi01001510	MSTP, MLT: When you attempt to enable STP learning on a MLT for an inactive MSTI, you may encounter an error message stating that the corresponding STP is not active, rather than stating that the MSTI is not active.
wi00982961	TACACS+, access mode log message: After connecting to the switch via Telnet/ console with TACACS+ enabled, the access mode log message indicates `no security`.
wi00989413	EDM, Stack Health: Display of switch stack health in EDM after units in stack are renumbered may not be accurate. **Workaround**: use ACLI command.
wi00992210	MAC Security address table: Static entry in the MAC security table should be created before planning to remove unit from stack.
wi00992287	MAC Security, MAC address table: If you have a MAC security list that has only ports from a unit which is no longer part of the stack, the MAC addresses that are statically associated with the MAC security list are not removed from the MAC address table, even though the MAC security list has been erased. **Workaround**: Manually remove the static entries.
wi00994307	EDM, IGMP: The 'in port' for IGMP groups is not displayed correctly in EDM. **Workaround**: Display in ACLI.

Change Request Number	Description
Resolved issues in Release 6.6.1	
wi00995161	RADIUS Management Accounting: When accounting is enabled/disabled from a Telnet/SSH session, NAS-Port-Type contained in the accounting packet is set incorrectly to Async, instead of Ethernet.
wi01001707, wi01001716	IGMP/SMLT: On stackable switches where Spanning Tree is enabled on VLANs/ ports, the following behavior can be expected due to the Spanning Tree convergence time. 1. There will be a 30 second delay of multicast traffic before traffic can be forwarded to MC clients connected on the base unit of the stack when a non-base unit is rebooted. 2. When the non-base unit rejoins the stack, there will be a delay of approximately 90 seconds before the multicast traffic can be forwarded to the multicast clients connected to the non-base unit. MC clients connected to the base unit experience the same behavior as in #1.
wi01004253	EDM, stack information: The display of stack information in EDM after booting the base unit may not be correct. ACLI should be used.
wi01007809	RADIUS accounting: When you log off a telnet/ssh session, the RADIUS accounting STOP session message sent indicates an incorrect Acct-Terminate-Cause of `Lost-Carrier` instead of `User-Request`.
wi01008960	EAP: If no more than 4 minutes and 30 seconds have passed after an EAP user is authenticated , a flush of the mac address table on the switch/stack will have no effect on the user`s authentication . However , if this timer expires , the client will try to re-authenticate and if it is still there it will get re-authenticated.
wi01009057	Security log messages: When you log out from an SSH session, you may see security log messages of `lost connection` instead of `user logout`.
wi01009215	AUR Auto-Save: The Auto Unit Replacement Auto-Save parameter value is not saved when autosave is set to disabled.
wi00993819	ADAC — ACLI-EDM inconsistency for UFB and UFA: If ADAC is configured as untagged frames basic or advanced, in EDM tagging appears to be enabled for phone ports, although tagging is disabled for phone ports from the view in ACLI. In ADAC untagged frames basic and advanced, LLDP policies on phone ports are untagged
wi01019181	The management traffic might be affected in a case where a static IPv4 route used for switch management from a remote network is more specific than a local route. To reestablish the management connection, the configuration of an IPv4 management route for the same network is required
wi01021166	MLT, MAC Security: When using MLT trunk ports with MAC-Security auto-learning and a set threshold (for example 20 out of 25 maximum possible value), bouncing the MLT trunk from enabled state to disabled state several times may cause the MAC SA entries learned to exceed the threshold.
wi01022088	EDM, MSTI: The error message `inconsistentValue` is displayed when trying to create an MSTI which already exists.

Change Request Number	Description
Resolved issues in Release 6.6.1	
wi01028882	SMLT/LAG: Currently in an SMLT over LACP scenario, the ACLI environment allows entering commands for binding multiple LAGs to the same SMLT ID. However, only one (the first one configured) binding becomes actually operational. Avaya recommends that you keep the LAG to SMLT ID bindings as one-to-one in order to avoid creating ambiguous device configurations.
wi01028979	PIM: The command `show ip pim interface enabled` may not return any of the enabled pim interfaces after a reset of the device.
wi01034689	EAP/NEAP, RADIUS: Using EAP/NEAP users with RADIUS assigned VLAN and fail open VLAN, authenticated users use RADIUS assigned VLAN. If the RADIUS server is unreachable, clients are moved in fail open VLAN. After defaulting to the RADIUS server, users are removed from fail open VLAN, while remaining authenticated. They will use RADIUS assigned VLAN. Reauthentication is not performed in this situation (EAP and NEAP clients are not flushed).
wi01035281	SMLT: Avaya recommends that you refrain from consuming all of the trunks 1-32 since configured aggregated trunks will utilize these starting at 32 and progressing through lower numbers (31, 30, 29, ...). Trunks may be configured using values of 33-512 and not create any conflict with trunks formed by aggregation.
wi01035284	LACP and mrouter ports are mutual exclusive. Avaya recommends using mrouter ports with MLT.
wi01035500	Brouter, IGMP Snooping: ip igmp snoop is not supported on brouter port. However, no error is returned when configuring it.
wi01035841	SLPP: If the '0' option is selected from the output of the `slpp timeout` command, the slpp timeout will be set to '4'.
wi01039420	Voice VLAN: If you encounter an Invalid Voice-VLAN ID error message while attempting to enable ADAC on a standalone switch which used to be part of a stack (even if the voice VLAN is set) check that the VLAN is a voice VLAN with command **`show vlan voice-vlan`**. If the VLAN does not appear in the list of voice VLANs, issue the command **`vlan voice-vlan vlan_id`** to enable ADAC.
wi01083893	IP Office Script - When configuring IP Office from edm-offbox or snmp, console lock and intermittent critical messages appear in syslog.
Resolved issues in Release 6.3.1	
wi01031886	The console locks up in diagnostics when downloading an agent and pressing **Enter** twice. Diagnostics software version 6.0.0.16 fixes this problem.
Resolved issues in Release 6.3	
wi00491923	The system does not remove all expired MAC Source Addresses in the MAC Address Table after the aging time has expired.
wi00484828, wi00492144, wi00497730	Device Type for devices connected to the data port on a VoIP phone are being displayed as UNKNOWN instead of PASSIVE in the command output of show nsna client.
wi00492820	ADAC port configuration types not defined in manual.

Change Request Number	Description
Resolved issues in Release 6.6.1	
wi00485407	Unnecessary system messages of STP_CLR_PCONFIG: PCFG_BRIDGING stpgId 0, portNo x are generated when disabling spanning tree on Ethernet ports.
wi00493682, wi00495091, wi00497859	Informational event type information is being sent to remote syslog server even when Event Type To Log is restricted to Critical and Serious event types.
wi00493706	No confirmation message is provided when an ASCII configuration, initiated via the UI (User Interface) push button, is successfully uploaded to the USB port.
wi00486074	Time Domain Reflector test ran from JDM is returning Pair Shorted as an error message for Pin Short cable problems rather than the correct error message of Pin Short.
wi00493776	MAC security Lifetime setting cannot be modified from the JDM.
wi00486100	MAC authorized clients are not reauthorized after a former base unit rejoins the stack.
wi00486318	LLDP configuration within an ASCII configuration file may fail to load during an ASCII configuration upload.
wi00486328	The cost metric, within the show ip routes output, for external routes increases to 127174722 when a fictitious OSPF virtual link is created than deleted.
wi00486432, wi00486962, wi00496973	The system does not remove user based policies nor age out the MAC addresses of Non EAPOL clients that physically migrate to a different EAPOL enabled port. This behavior will result in Non EAPOL authentication failure for migrating clients when attempting to authenticate and applying policies on their new ports. Error state will generate the following system messages: Duplicate users (different port, same user name) and bsnEapUbpFailure prohibited.
wi00486497	Unknown multicast and known multicast variables within a system classifier are not functioning correctly. Issue is exclusively on the 5600.
wi00486386	Multicast traffic is not forwarded to the destination network configured within a non-local static route (NLSR). A NLSR is similar a regular static route except that the next hop of a NLSR static route is not directly connected
wi00486635	The source IP address for traffic destined for a RADIUS server should be the IP address of the Management VLAN IP interface.
wi00494290	PIM is intermittently being disabled on random VLAN interfaces after a reboot.
wi00494367	Incorrect error message of "Invalid file name" is being generated when attempting a software download from an unreachable server.
wi00486652, wi00488134, wi00489324, wi00496995	Uploading an ASCII configuration containing IP route commands results in configuration upload failure and the following system messages: % Cannot modify settings % Duplicate Route Entry. Use Modify Operation
wi00494385	IPv4 and IPv6 IP Addresses stored within NVRAM are not overwritten by the IPv4 and IPv6 Addresses existing in the ASCII configuration file being uploaded to the unit/stack.

Change Request Number	Description
Resolved issues in Release 6.6.1	
wi00486691	Some ARP, OSPF, or VRRP packets are unexpectedly mirrored when using XrxYtx mirroring mode and the monitored port is in the Management VLAN or in SMLT VLANs.
wi00486687	MAC addresses are lost when a base unit fails.
wi00486701	LLDP-Med fails to configure VoIP phones with defaulted configuration. VoIP fails to initiate displaying error messages of "Starting DHCP..." or "DHCP server unreachable..".
wi00486698	ADAC syslog messages sent by non base units is displaying ADAC: System operationally during a system reboot. During a system reboot ADAC is down. The base unit sends the correct syslog message of ADAC: System operationally dis abled
wi00486715	On a pure 56xx stack, port mirroring mode XrxYtx multiplies unicast traffic on port Y in certain scenarios.
wi00486712	Disabling and re-enabling VLACP followed by a reboot will result in VLACP failing to function after the system restores from a reboot.
wi00486688	The EAP-TLS or PEAP-MsChapV2 clients could be unexpectedly transitioned to the EAP Held state on a multihost enabled port.
wi00486710	Voice traffic is blocked on a non-base unit when ARP inspection is enabled on a VoIP VLAN.
wi00494406	Walking the ipNetToPhysicalPhysAddress MIB results in a system reboot with various data access exception tasks of tLDT, tSNMP or bcmRX.
wi00494771	The LLDP Med-Network-Policies Voice Tagging command is rejected and deemed invalid by the operating system when attempting to execute the command.
wi00494479	PIM outgoing interfaces may not be installed in the r × r identity matrix (IR) if session directory tool (SDR) is flapped.
wi00494624	Continuous IPv6 ping stops working after 2147 ICMPv6 messages.
wi00486941	Telnet session hangs on ERS 5510-48T during an ASCII configuration download.
wi00487092	ACG fails to function if a ports tagging mode is Untagpvidonly and the port is also member of 2 Spanning Tree Groups.
wi00494933	After booting to default setttings the syslog will display the message **`ASCII failed at line 1`**. This can be ignored. This only happens after a boot to default settings and not during a normal operation or reset of the switch. This does not affect subsequent ASCII downloads. The successful application of configurations can be confirmed using the **`show logging`** command. The bogus message will be the first in chronological order.
wi00992380	The correct argument order when uploading the sshc key to an usb device and specifying a certain unit is :**`sshc upload-host-key usb unit 1 key-name word dsa`**.

Chapter 5: Known issues and limitations

Use the information in this section to learn more about known issues and limitations. Where appropriate, use the workarounds provided.

Known issues

See the following table for a list of known anomalies for the Avaya Ethernet Routing Switch 5000 Series.

Table 4: Known issues

Change Request number	Description
Known Issues from Release 6.6.1	
wi01142882	Lossless - Background traffic is dropped and error messages appear on CLI.
wi01161272	Auto Qos Granularity - l3 traffic is limited too soon, not after the expected interval.
wi01170165	Unauthorized hosts are able to receive IP from DHCP Server.
wi01176631	STP - STP state not saved after bu reset.
Known Issues from Release 6.6	
wi01067057	Downgrading software release - if you downgrade from 6.6.0 to /6.0.z/6.1.k/6.2.x/ 6.3.w you will lose the configuration, i.e. the configuration is erased. Configuration is lost when device ERS 5000 is downgraded to lower version.
wi01081912	TDR - pairs of wires are incorrectly displayed as swapped after a TDR test on straight through or crossover cables.
wi01083597	IP Netstat - Local and foreign addresses may be incorrectly displayed by the show ip netstat command when using TFTP transfer.
wi01087989	EDM, multiport - mcast/bcast may not be set correctly in EDM when applying configuration on all ports.
wi01092387	SSH Client, banner - an incorrect banner may be displayed after connecting to the switch via SSH Client.
wi01092410	UI Button - with the Default IP feature, the UI button no longer has the ability to set the default IP address. You can continue to configure IP paramenters using the console menu and ACLI command `ip address` or in EDM from the Administration > Quick Start menu.

Change Request number	Description
Known Issues from Release 6.6.1	
wi01092748	DSA Key Generation - Generation of DSA key takes much longer from Telnet and SSH than from CLI. DSA key generation from CLI takes approximately two seconds, whereas Telnet ranges from 20–30 seconds, and SSH approximately 60 seconds.
wi01094184	BGP - total imported routes count is doubled after restarting BGP and is not cleared after disabling redistribution.
wi01095251	SNMP, CLI - if you continuously poll the MIBs related to PoE on PWR units, the CLI response time increases on those units. Response time recovers when the polling of the MIB set is complete.
wi01095692	DHCP Snooping - When the DHCP client sends DHCP release to a DHCP server, only one syslog message is generated for a DhcpSnooping trap, instead of two. No syslog message is generated when the switch sends bsDhcpSnoopingTrap.
wi01096361	IPMGR - IP Manager configuration is not available when managing the device through COM (EDM-Offbox). The Configuration\Administration\Remote Access is grayed out even if discovering the device using a high security SNMPv3 user. This configuration will only be possible through a direct EDM connection.
wi01099044	OOB Management, CLI password type - CLI password type TACACS+ doesn't apply with only out-of-band management IP configuration. If using RADIUS instead of TACACS+, CLI password type changes to RADIUS as expected.
wi01101091	QoS - For CIR equal to 64000 or 128,000 kbps, the traffic isn't limited after the expected period of time, calculated based on the confiugred committed rate and burst size, when sending traffic with a higher rate than the CIR. The actual burst duration is up to double the expected burst duration.
wi01102781	DHCP- DHCP packets may be displayed as filtered when DHCP Snooping is enabled, but the IP address can be obtained from the server.
wi01103115, wi01103120	IST core reboot - the recovery time in the case of an IST core reboot will be approximately 15 seconds.
wi01111136	OOB Management - Ping in a directly connected network does not work from the switch when a less specific route for the same network is configured through out-of-band management.
wi01111419	TBU reboot - the console may be flooded with debug messages when the Temporary Base Unit is rebooted.
wi01112588	VRRP, DHCP - DHCP packets are doubled in an SMLT with VRRP scenario.
wi01112641	OOB Mgmt, EDM/COM - you cannot administratively enable or diable the out-of-band port from EDM/COM. A command for this functionality is available in CLI.
wi01115099	FOV Continuity - additional Fail Open VLAN Continuity mode syslog messages may appear due to checks performed on individual client request. These messages do not reflect the final state of the ports involved.
wi01116959	LLDP, EDM - LLDP MED network policies are not created from EDM if the port is not a member of the VLAN.

Change Request number	Description
Known Issues from Release 6.6.1	
wi01117600	Voice VLANs, ADAC - if a port is configured with both ADAC and EAPOL voice VLANs, when the ADAC op-mode is modified, the port is removed from all EAP voice VLANs and remains only in the ADAC voice VLAN.
wi01121469	LLDP port TLVs - MgmtAddr lldp tx-tlv is not present in EDM TLVsTxEnable tab (Edit->Diagnostics->802.1AB->LLDP->Port tab). In ACLI it is displayed next to PortDesc, SysName, SysDesc, SysCap, under the `show lldp tx-tlv` command.
wi01122505	EDM offbox, LLDP Avaya Local File Server - an error message is received when attempting to access the configured LLDP Avaya Local File Server.
wi01122965	COM/EDM Offbox - Unavailable options from non-default VRF navigation tree are not greyed out. Only IP-> IP, IP-> DHCP Relay, and Help should be available.
wi01124972	QoS - Configuration of the 128th byte of a QoS system element is not possible. If using up to the 127th byte, configuration is properly applied.
wi01124975	QoS - QoS system elements matching more than two chunks having different pattern data in the same position cannot be applied on the same if-group.
wi01127017	PIM - Incorrect PIM join-prune-interval and query-interval values are displayed and saved in config. The ‘default’ command does not restore the parameters. You can manually re-enter the parameters.
wi01131174	EDM, Change RADIUS password - access to EDM is granted even though an incorrect password format is used when changing the RADIUS password in EDM.
wi01131178	EDM, Change RADIUS password, Firefox - after successfully changing the RADIUS password from a Mozilla Firefox browser through EDM, the log on button is missing from the top of the page.
wi01131546	DHCP Snooping, EDM - EDM displays ‘noSuchObject’ for SftpServerAddress in DHCP Snooping Global folder on non-SSH agent image.
wi01131924	EDM, Change RADIUS password - when changing the RADIUS password from EDM after the account is marked for a password change, the switch allows you to use the same set of credentials.
wi01131927	EDM, Change RADIUS password, Firefox - when changing the RADIUS password from EDM after the account is marked for a password change, hitting the Enter button has no effect using Mozilla Firefox.
wi01131934	EDM, Change RADIUS password - when changing the RADIUS password from EDM after the account is marked for a password change and refreshing the page, the login is permitted without entering any credentials.
wi01132500	EDM, IPv6 icmp - you cannot enable/disable IPv6 icmp block-multicast-replies from EDM. This functionality exists in CLI.
wi01134096	SSH - SSH connection may fail to establish while a binary configuration is being saved.
wi01135843	Stack Monitor - Stack Monitor traps are not correctly sent at every trap-interval when one unit from a stack is removed.

Change Request number	Description
Known Issues from Release 6.6.1	
wi01136733	EDM, STP BPDU-Filtering - EDM displays an incorrect error message if you enter an out-of-range value for STP BPDU-Filtering Timeout field.
wi01136918	EDM, Change RADIUS password, Firefox - when using EDM from Firefox version 3.6.2, after the account is marked for a password change, the previously entered username and password disappear.
wi01138196	show ip rip ACLI command - the switch returns 'Internal Error' for the ACLI command `show ip rip interface ethernet` on units with specific configurations. As a workaround, use the ACLI command`show ip rip interface vlan`.
wi01140365	Lossless mode - if running in lossless mode, ensure that flow control is set to asymmetric or symmetric on the switch and the connected neighbors.
wi01141450	SNMP, IPv6 – SNMP walk is interrupted if default IPv6 route is enabled and appears in the IPv6 route table. Workaround: disable the IPv6 default route, remove it, or use a more specific route. For example, `ipv6 default-gateway 4148:4:4:340::1`, `no ipv6 route ::/0 next-hop 4148:4:4:340::1 vlan 3927 enable`.
Known Issues from Release 6.3.1	
wi01074793	IP Office Script - run ip office script fails if switch or stack management IPv6 address is configured.
wi01088633	If the default vid = 0, then the default LLDP med-network-policies aren't sent from DUT. As a protective measure, if the LLDP-MED network policy has VID = 0, then the switch does not advertise the network policy TLV (even if the policy is enabled); for all other values of VID, the switch sends out the advertisement.
wi01067057	The configurations on the switch are lost after downgrade because binary configuration files can only be loaded in same build it was saved. **Workaround:** To fix this Binary configuration issue, the software erases both the memory blocks of NVRAM before reloading the downgrade image and blocks are set to default configurations. If the configuration is required on downgrade, then save the configuration to ASCII and restore it once the downgrade to the required software is completed.
WI01088875	In the EDM Help, the IP Route to Gateway Modem-Router (Internet/WAN) default value is 192.168.43.2 This value should be: Default IP Route set to 192.168.44.2 (Gateway Modem-Router interface).
Known Issues from Release 6.3	
wi00906543	EDM, 10G Ports: 10G ports are not seen in EDM under Power Management > PoE > PoE Ports.
wi00927200	NEAP, MHSA Configuration: When a disconnect message is sent for an authenticated EAP user in MHSA mode, you may experience a 15 second delay before the port reverts to the initial VLAN (or Guest VLAN).

Change Request number	Description
Known Issues from Release 6.6.1	
wi00932580	NEAP, EAP clients and bsnEapRAVError trap: The bsnEapRAVError trap is generated only for EAP clients and not for NEAP clients.
wi00933750	RIP out policy: RIP out policy using network prefix to drop specific networks will not forward other route networks learned from OSPF, static, and direct routes. **Workaround**: Make a sequence 2 in the same route policy to forward any protocol.
wi00960304	EDM, ip-fwd-nh policy: When you create an ip-fwd-nh instance from the base unit using EDM, the policy may fail to attach to a port based VLAN.
wi00983765	SSH Banner has only ACLI support (no EDM support).
wi00987283	USB devices: USB devices with NTFS or exFAT file format are not supported. FAT32 is the only supported file format.
wi00995161	RADIUS Management Accounting: When accounting is enabled/disabled from a Telnet/SSH session, NAS-Port-Type contained in the accounting packet is set incorrectly to Async, instead of Ethernet.
wi00996182	TBU, MLT: In a stack configuration, MLT trunk members for units that are temporarily not part of the stack (for example in a reboot process) are still attached logically in the configuration of active units. This event will not show aggregated ports as they will be dynamically hidden in CLI and ACG while the missing unit is not available.
wi01000569	SNMPv3 user: When you create a new SNMPv3 user with password security disabled, using a password string within the required length but with an atom that repeats twice (for example, the password string '12341234'), the user will not be created.
wi01007577	DHCP Snooping filename: The maximum length of the DHCP Snooping external filename varies between ACLI and EDM.
wi01009777	IPFIX — EDM-Offbox: You may be unsuccessful in applying settings for a large number of ports from EDM-Offbox on a SNMPv3 discovered device. Reducing the number of selected ports will yield the expected result.
wi01038367	SSL Certificate/RSA key generation: When the switch generates an SSL certificate at the same time the RSA host key is generated, the CPU may be busy for a short time, as the two activities can be resource intensive.
wi00935460	LACP : When booting a system with one or several LAGs configured, the trunk IDs of the LAGs might not be the same after the system comes up again. The only way to predict this is on an SMLT-LACP environment where the LAG ID is bound to an LACP key
wi00983785	Security, Dynamic ARP: When Dynamic ARP Inspection is configured and ARP packets with invalid IP/MAC bindings are received on untrusted ports, traps may be generated for the first port on the corresponding unit on which the invalid ARP packet is received.
wi01010916	QoS: Disabled but not deleted QoS policy data can impact resource utilization. Avaya recommends that you delete QoS policy data that is not required for long term configuration, as opposed to simply disabling the QoS policies. If you experience unexpected resource allocation issues and disabled QoS policies are

Change Request number	Description
Known Issues from Release 6.6.1	
	present, the initial step towards alleviating the resource issue is to delete the currently disabled QoS policies
wi01020873	IGMPv3: IGMPv3 traffic is doubled when port mirroring is configured to mirror the mrouter port on the L2 device (with IGMPv3 snooping enabled) on which the IGMP receiver is connected. You may experience this issue with port mirroring modes: Xrx, XrxOrXtx, manytoOneRx, manytoOneRxTx.
wi01028901	L2, SMLT: On stacks that are involved in IST configuration with the IST links being VLACP enabled with a short time-out value, VLACP brings down the IST during the stack formation process due to lack of VLACPPDUs received. After the rebooted stack is formed again, the IST recovers as soon as VLACPPDUS are received. Workaround: Set a timeout-scale timer value larger than 6.
wi01030591	EDM, QoS statistics : When using QoS statistics for Traffic Profile from EDM, EvalOrder will not be correctly shown on ports from non-base units if the same Traffic Profile set uses multiple eval orders (non block configuration). QoS statistics work as expected on ports from the base unit.
wi01030811	Filter Limiting: Settings made while filter limiting is disabled (more protocol filter entries) are not seen when filter limiting is enabled (fewer protocol filter entries), but the entries are retained. When filter limiting is subsequently disabled and the switch/stack is rebooted, these retained entries will be activated unless changes made while filter limiting was enabled have created conflicts with the retained entries. You do not typically need to switch between settings. If you do, and at the same time you are changing the protocol VLANs, you need to exercise caution or the results when filter limiting is disabled may not be as expected. Changes made while filter limiting is enabled will override those that are retained in the expanded protocol filter list.
wi00946819	Port name is limited to 64 characters in both ACLI and EDM.
wi01004362	Security 802.1X EAP: In a scenario where an IP Phone and a PC behind the phone are connected into an EAPOL multihost enabled port and only the IP Phone is successfully authenticated, starting a ping over IPv6 into the system's management VLAN's IPv6 address will succeed even if the PC is not successfully authenticated. However, all other IPv4 and IPv6 traffic not destined for the switch will be dropped.
wi00945013	SNMP: SNMP inform traps are not generated correctly by the switch (both header and PDU variable bindings) and will fail to be interpreted by the receiving SNMP trap daemon host.
wi00962526	AAUR: When carrying out the AAUR process in a pure Waverunner stack, the message `NVR CFG - Could not acquire FLASH sem` will be registered throughout all units of the stack. There is no impact on the AAUR process which will be successful.
wi00925548	DecOtherEther2, Filter Limiting: When Filter Limiting is disabled and configured to use additional filter slots (beyond 7), the saved ASCII configuration will include the additional VLANs which are defined using the extended filter slots. If a switch/stack is reset to defaults, it will come up with Filter Limiting enabled and will now be limited to 7 filter slots. VLANs which are defined for the additional slots will fail to be configured on the switch. The use of a DecOtherEther2 protocol VLAN will fail since

Change Request number	Description
Known Issues from Release 6.6.1	
	it requires 10 protocol slots. If a configuration is using the slots provided by disabling filter limiting, you must disable filter limiting via ACLI and reboot the switch/stack before applying the ASCII configuration so that it is operating in the Filter Limiting disabled mode.
wi00930131	SLPP Guard: The ACLI command **`no slpp-guard`** disables slpp-guard on a specific port **`(no slpp-guard port X enable)`** or disables the auto re-enable timeout **`no slpp-guard port X timeout)`**. If neither parameter is specified (**enable** or **timeout**), both settings will be disabled, i.e. slpp-guard is disabled and the timeout set to 0 on the specified port(s).
wi00987107	EDM, Rate Limiting: When configuring rate-limit settings for switch ports using EDM, setting pps or percent for either the broadcast or multicast traffic type will trigger the both parameter to apply for the port selection.
wi01016205	When initiating an eapol init on a port with authenticated EAPOL users that have associated DHCP-clients leases that populate the dhcp-snooping binding table, users will be de-authenticated but former entries may still populate the dhcp-snooping binding table. You can issue a manual clear mac-address table command.
wi00945962	VRRP: If you encounter the message `% Not enough HW resources available` when enabling VRRP, try again after a 30 second interval. This may result from high CPU utilization.
wi01030857	MAC Security, EDM: The MAC-Security "MacViolation" tab from EDM will not list any intruder mac-addresses as expected.
wi00973591	Even though the image has been downloaded successfully and the continuous ping was not interrupted the following messages are displayed intermittently : `Request time out!` The connection with the device may be lost or the device may be down.
wi00974433	RADIUS key for secondary servers (GRS/ERS/NRS) is deleted when defaulting primary server. Is recommended to use "no radius server host" instead of "default radius server host". This way, if a secondary server is configured, the key will remain in use for that secondary server.
wi00973591, wi00975529	RADIUS dynamic server clients statistics may not be seen when using EDM Offbox.
wi00978991	EDM, BGP: When creating a community list or As path list from EDM, with member id greater than 10, the list will not be displayed correctly from EDM.
wi00984496	EDM System up-time: Stack info uptime seen from EDM does not display uptime for non base units.
wi00993182	EDM, LACP: In EDM, sorting the trunks in the Vlan->MLT/LACP section is possible only for the MLT tab.
wi01005364	DHCP, reboot: After reboot, DHCP requests from client pass the switch port before MAC authentication(radius-request) starts. The device receives an IP address of the Guest VLAN , even if the client is eventually authenticated and moved to initial / radius vlan .This scenario is reproducible only when clients are simulated by traffic

Change Request number	Description
Known Issues from Release 6.6.1	
	generators; the issue is not reproducible in a real case scenario (client = PC / IP Phone)
wi01013703	EDM, IST: IST may not be enabled when EDM is used. Workaround: Enable IST from ACLI.
wi01018390	COM: The following message is displayed, even though the connection is not lost. `Request time out!` The connection with the device may be lost or the device may be down.
wi01021894	LLDP: In version 6.3, the LLDP default settings for lldp tx-tlv and lldp tx-tlv med have been changed to enabled. In prior releases, the default setting for LLDP was disabled. These settings only apply when the switch is defaulted or the default LLDP setting is applied. When upgrading from a previous version, the configured LLDP settings will be retained.
wi01022549	When the device reaches a situation in which it sends out an ICMP Destination Unreachable message through a specific port, the icmpOutDestUnreachs.0 counter should be increment each time such a message is sent. Currently this counter is not incrementing properly so it is best to rely on capturing such packets if required for a traffic statistic.
wi01024984	The error message `% TFTP server address has not been set` is intermittently displayed for the command `configure network`.
wi01027416	SNMP: The error message `commit failed` is returned when a user tries to disable the STG of the management VLAN using SNMP.
wi01027752	Multicast traffic might be lost after maximum of multicast routing entries(992(*,G)and(S,G)) are learned on WR stacks.
wi00931239	EDM, Rate-limit: When configuring rate-limit from EDM on a multiple port selection, desired values may sometimes not be applied as expected. The same options can be set from ACLI.
wi00980212	OSPF, MAC security: Avaya recommends you do not use MAC security on OSPF enabled links on 5520 and 5530 units.
wi00555204	ADAC and LLDP policies: A user-configured LLDP-MED network policy takes precedence over an ADAC auto-configured LLDP-MED network policy, and will overwrite an existing ADAC policy. Since ADAC policies are dynamically auto-configured, if you delete the previously configured policy, the ADAC auto-configured policy is not restored. For the ADAC auto-configured policy to be reapplied, you must unplug and then plug in the IP phone in order for the ADAC auto-discovery and auto-configuration process to take place again.
Known Issues from Release 6.2	
wi00484542	In an NSNA setup, you may experience temporary loss of NSNA functionality when UDP forwarding has approached maximum capacity. Workaround: Configure a filter on the port that connects to the SNAS (or depending on your configuration, on the port connected to the switch that, in turn, connects to the SNAS) to isolate NSNA SSCP traffic received by the CPU. Use the following CLI commands to configure a filter:

Change Request number	Description
Known Issues from Release 6.6.1	
	qos ip-element <element_id> src-ip <ip_address/mask> **qos classifier <value> set-id <value> element-type ip element-id <value>** **qos action <value> update-1p <value>** **qos policy <value> port <port_list> clfr-type class clfr-id <value> in-profile-action <action_id> prec <value>**
wi00486677	It may take more time than usual for traffic to re-converge (approximately 10 seconds) if a stack from the core is rebooted in a highly scaled SMLT configuration (100 VLANs).
wi00494404	Port mirroring mode XrxYtx on a 56XX device does not mirror broadcast, multicast and unknown unicast traffic if the X and Y mirrored ports are in different MLTs.
Q01979384-01	HTTP connections are not displayed by the **show ipv6 tcp connection** command.
wi00486821	The **show ip ospf neighbor detail** command that provides detailed information for OSPF LSDB should not be run when the terminal length is set to 0.
Q02004055	There is currently no command to disable the **metric** and **route-type** options for the **route-map <route_name> match** command and no command to disable the **ip preference**, **metric**, and **metric-type** options for the **route-map <route_name> set** command.
wi00494595	Specifying a range of ports for non-base units using the **poe poe-shutdown port X** command may cause IP Phones connected to those ports to remain powered on in some stack configurations.
wi00486898	Wait twice the configured MAC aging time after swapping two PCs behind 2 phones in an NSNA solution before plugging the PCs back in behind the phones.
wi00494935	If the UBP set is configured and the QoS agent is disabled when an EAP / Non EAP user authenticates, several log messages displaying **QoS support is currently disabled** will be produced.
wi00487438	OSPF: Even though two LSA packets are sent (one with unicast destination address and one with multicast destination IP) only one LS ACK transmitted packet appears in the interface statistics table.
Q02056133-02	EDM: to enable or disable EDM access use ACLI commands **web-server enable** or **web-server disable**.
wi00495084	STP is re-enabled when moving SMLT ports from 1 STG to another.
wi00484360, wi00487405, wi00497106, wi00554983	Stacking: When you copy a binary configuration to an TFTP server, you may receive an `Intra-stack communication failure` message. This does NOT indicate a stack failure; it indicates that the command failed. **Workaround**: : If you receive the `intra-stack communication failure` message, execute the **copy binary** command until it succeeds.
wi00495158	In the SMLT network, loop may be temporarily introduced on LACP-over-SMLT port. In order to prevent loop from happening it is required to configure all LACP-

Change Request number	Description
Known Issues from Release 6.6.1	
	over-SMLT port in "Lacp Advance mode". Under this mode, LACP port stays in Blocking mode until it receives the first LACP PDU from its partner port. In 6.2 release, it is the user's responsibility to put all LAC-over-SMLT ports in "Lacp Advance Mode.
wi00488453	Do not see the ability to set Forced Stack Mode via the EDM interface.
wi00495698	SFPs: To ensure a proper match of the remote side, before you install an SFP set shared ports to auto-negotiate. Refer to ACLI: default speed and default duplex
wi00495332	IPv6 Tunnel over IPv4 operational status is determined by combination of IPv6, IPv4 forwarding, and VLAN status. The IPv6 tunnel operational status is ACTIVE if IPv6, IPv4 forwarding is enabled and the VLAN status to which source IPv4 tunnel end point is UP (i.e. at least one port on VLAN is connected). Operational status ACTIVE does not indicate the liveliness or reachability of IPV4 remote tunnel end point.
Q02089575	Supported capabilities in Ethernet Routing Switch 5000 Series switches, the maximum supported PIM-SM entries should state up to 492 for 55xx Switches and up to 992 for 56xx Switches - not 500 and 1000.
wi00484056, wi00487793, wi00497158	TDR: Run TDR tests only for ports with Link Status UP.
wi00484096, wi00488154, wi00497196	`show running-config defaults` When you execute the show running-config defaults or show running-config default specific commands the system may take up to 4 minutes to return results, depending on the complexity of the system: for example, an 8-high stack fully configured. This is considered normal behavior.
wi00496125	The old RSTP Traps command is hidden (this means is not displayed when question mark is given and the command is not autocompleted when hitting TAB). Use the new commands found under 'snmp-server notification-control'. You can obtain a list of the current notification traps available using 'show snmp-server notification-control'.
wi00487670	IPv6 DHCP Relay does not support Remote ID parameter (RFC 4649) in this release.
wi00488121	EDM, RATE LIMITING: Multiple port configuration for Rate Limiting may not work properly; the change allow rate of broadcast or multicast may produce an incorrect result. WORKAROUND: Use ACLI to configure Rate Limiting.
wi00495711	In Lossless mode, when oversubscription exceeds 10 ports to 1 port, ingress ports must be spread across groups of 24 ports.
wi00496306	Energy Saver: When energy saver is activated or deactivated, the link on a port briefly transitions. This causes some devices to re-acquire connectivity. For copper uplink ports or critical devices, it is recommended to disable energy saver at the port level.

Change Request number	Description
Known Issues from Release 6.6.1	
wi00496308	EAP authentication will be restarted on copper ports when Energy Saver transitions to active or inactive state. This occurs because Energy Saver is clearing the MAC address on the EAP client port when transitioning to the active or inactive state. EAP fiber port status does not change when Energy Saver is activated or deactivated.
wi00496309	NEAP authentication is restarted on copper ports when Energy Saver transitions to active or inactive state. This occurs because Energy Saver transition clears the MAC address on the NEAP client port. NEAP fiber ports EAP status does not change when Energy Saver is activated or deactivated
wi00487721	PORT MIRRORING: Port mirroring will mirror pruned multicast streams to the monitor port. However, the streams are not actually sent to the device because they are pruned.
wi00555143	Upgrade: All trap notifications are enabled after you upgrade to R6.2.0 software, regardless whether you disabled them prior to the upgrade. For procedures to restore trap functionality, see Trap restoration and reconfiguration after upgrade to Release 6.3 on page 48.
wi00496317	ROUTING, DEFAULT GATEWAY: If you enable and disable routing globally on the management VLAN the default gateway may not work. In R6.2 you can configure the switch with default gateway (using the command **`ip default-gateway <next-hop>`** or default route (using the command **`ip route 0.0.0.0.0.0.0.0 <next-hop>`**) . When IP Routing is disabled (Layer 2 mode) on the switch, the default gateway serves as the default route, that is the default gateway shown by the **`show ip`** command. When IP Routing is enabled (Layer 3 mode) on the switch, the default route specified is used, that is the 0.0.0.0 route shown by the **`show ip route`** command. You can enter up to 4 static routes, management static routes, to be used for management traffic only. These routes are used in software routing only and do not affect pure data plane traffic. SOLUTION: You must enable routing on the management VLAN to activate management static routes which you can use for separation of management and data traffic.
wi00488714	LLDP MED NETWORK POLICIES: You cannot assign custom DSCP values to Avaya 1120E IP Deskphones using LLDP MED network policies.
wi00491740, wi00496258, wi00498185	It is recommended that you use SNMPv3 to achieve security, instead of using SNMPv1 and/or SNMPv2c with community strings.
wi00554875, wi00555204, wi00555283	802.1ab MED: Both LLDP MED and ADAC policies are supported on the same port. If both types of policies are created on the same port and you delete the LLDP policy you created, then the ADAC policy is also deleted.

Change Request number	Description
Known Issues from Release 6.6.1	
wi00554955	IPv6 Static Routes: In an IPV6 setup where static and backup static routes exist, if you disable the IPv6 routing on a neighbor next-hop router, the active route will remain active until ARP for the next-hop expires or until a neighbor solicit message is forced (ping, clear neighbor, clear neighbor mac address) or until you execute shutdown/noshutdown on the respective interface.
Q02149708	Energy Saver: You must not select fiber ports when you use the Multiple Port Configuration menu to enable Energy Saver on a range of ports.
Q02150634	AUR/DAUR: The reboot process can take approximately 3 minutes to complete, after which the normal CLI commands will display the AUR status.
wi00555132	AUR, LICENSING: After you perform automatic unit replacement (AUR) of a base unit, if the MAC address of the new unit introduced into the stack was not part of the original license, then, when you reboot the stack and execute the ACLI command **`show license all`**, the output displays that 0 licenses are present. WORKAROUND: Licenses will be operational, or can be enabled, and you can verify the license state using the following ACLI commands: • **`show license all verbose`** to check whether any bit is set in the License Vector in Use data • **`show sys-info`**: the Operational license field shows the current license state • **`show system verbose`**: Operational license field shows the current license state
wi00933491	802.1AB MED network policies: Avaya IP phones may not apply LLDP MED network policy configurations received from the switch on older phone firmware versions.
wi01008592	LLDPDU and TLV error handling: in the scenario where you have a large number of VLANs configured and dot1 port-protocol-vlan-id and vlan-name TLVs are enabled, TLVs may not be transmitted. With the maximum size of an LLDPDU packet at 1518 bytes, some TLVs such as dot3, MED, and vendor specific Avaya TLVs may not be sent.
wi00934940	LLDP Integration: on the Avaya IP phones, the Current Conservation parameter is not set according to the PoE conservation level request TLVs.

Trap restoration and reconfiguration after upgrade to Release 6.3

Use the procedures in this section to restore and reconfigure trap functionality after you upgrade to Release 6.3 software. You can reconfigure trap notification, using either EDM or ACLI.

Restoring trap notification functionality using ACLI

About this task

Use the following procedure to restore trap notification functionality using ACLI:

Procedure

Use the following ACLI command to remove traps created using R6.1 and before: **`no snmp-server host X.Y.Z.T ‘community name’`**

Reconfiguring traps using EDM

About this task

Use the following procedure to reconfigure traps using EDM:

Procedure

1. From the navigation tree, click **Edit**.
2. From the Edit tree, click **Snmp Server**.
3. In the work area, select the **Community** tab.
4. Create a community string - you must specify the Notify View name.
5. In the work area, select the **Host** tab to create an SNMP host - use the community you created in the previous step.
6. On the **Host** tab, use the **Notification** button to activate or deactivate individual traps.
7. In the work area, select the **Notification Control** tab to activate or deactivate individual traps per device.

Reconfiguring traps using ACLI with v1 host example, password security enabled

About this task

Use the following procedure to reconfigure traps using ACLI - v1 host example with password security enabled:

Procedure

1. To create a community, from the Global Configuration prompt, enter the following command:

   ```
   snmp-server community notify-view nncli
   ```

   Enter community string: CommunityName

   Enter community string: CommunityName

2. To create an SNMP host using the community you created in the previous step, from the Global Configuration prompt enter the following command: `snmp-server host 10.100.68.3 port 162 v1 CommunityName filter TestFilter`.

Reconfiguring traps using ACLI with v1 host example, password security disabled

About this task

Use the following procedure to reconfigure traps using ACLI - v1 host example with password security disabled:

Procedure

1. To create an SNMP community, from the Global Configuration prompt, enter the following command: `snmp-server community CommunityName notify-view nncli`.
2. To create an SNMP host using the community you created in the previous step, from the Global Configuration prompt enter the following command: `snmp-server host 10.100.68.3 port 162 v1 CommunityName filter TestFilter`.

Setting the Notification Type per receiver using ACLI

About this task

Use the following procedure to set the Notification Type per receiver using ACLI.

Procedure

1. From the Global Configuration prompt, enter the following command: `snmp-server notify-filter TestFilter +org`.
2. From the Global Configuration prompt, enter the following command: `snmp-server notify-filter TestFilter -linkDown`.
3. From the Global Configuration prompt, enter the following command: `snmp-server notify-filter TestFilter -linkUp`.

Displaying Notification Types associated with the notify filter using ACLI

About this task

Use the following procedure to display the Notification Types associated with the notify filter using ACLI.

Procedure

From the Global Configuration prompt, enter the following command: `show snmp-server notification notify filter`

Enabling or disabling the Notification Type per device using ACLI

About this task

Use the following procedure to enable or disable the Notification Type per device using ACLI.

Procedure

1. From the Global configuration prompt, enter the following command: `no snmp-server notification-control linkDown`.
2. From the global Configuration prompt, enter the following command: `no snmp-server notification-control linkUp`.

Preventing a loop during upgrade of a large network

About this task

Use the following procedure to prevent a temporary loop during upgrade of a large network.

Procedure

1. Shut down LAC/SMLT ports on system A.
2. Download the new software image to system A.
3. Enable LAC/SMLT ports on system A.
4. Shut down LAC/SMLT ports on system B.
5. Download the new software image to system B.
6. Enable LAC/SMLT ports on system B.

Ethernet Routing Switch 5000 Series limitations and considerations

The following table lists known Ethernet Routing Switch 5000 Series limitations and considerations:

Table 5: Ethernet Routing Switch 5000 Series considerations

Item	Description
1	Some terminal programs can cause the Console Interface to crash if you enter a RADIUS secret containing the character “k”. The issue has been reproduced using Tera Term Pro (version 2.3), as well as Minicom (version 2.1) on a Linux system.
2	Avaya recommends that you avoid using MAC security on a trunk (MLT).
3	Failed attempts to log in (using TACACS+ authentication and accounting) are not stored in the accounting file.
4	When switches are in MSTP mode and connected using a trunk (MLT), and at least one MSTI is configured, the switch can return an incorrect STPG root if you change the mode to STPG and reset the switches.
5	When you use the EDM/Web to configure and add VLAN ports to an STG other than the default STG, STG membership of the port may change. In that case, the new STG participation of that port will be disabled. WORKAROUND: Enable participation of the ports in the new STG after you enable the STG.
6	While downloading the image file, you may receive the following error message: "Error reading image file." WORKAROUND: Typically, this issue can be resolved by simply restarting the image download. If this does not resolve the issue, Avaya recommends that you try an alternate method to download the image to the switch (that is, the Web Interface).
7	The IPFIX sampling data rate cannot be changed because of a related hardware limitation.
8	Release 5.1 introduced a Demo License to enable OSPF, ECMP, VRRP, SMLT, and IPFIX for a period of 30 days. The trial license expires at the end of the 30-day period and the features, except SMLT, are disabled. The system sends traps advising of license expiration but SMLT remains enabled until the stack or unit is reset. Avaya recommends that, when you receive the first trap, the administrator begins to manually disable SMLT and ensure removal of any cabling loop. Because Spanning Tree Protocol needs to be disabled and, because SMLT is implemented through cabling, SMLT is not disabled with the other features because a network loop would form. After demo license expiry, when the stack or unit is reset, SMLT is disabled and a loop will form if there has been no intervention to remove or disable the ports participating in the IST. Demo license expiry traps: Five days prior to demo license expiry: bsnTrialLicenseExpiration: Trial license 1 will expire in 5 day(s). One day prior to demo license expiry: bsnTrialLicenseExpiration: Trial license 1 will expire in 1 day(s). At termination of demo license: bsnTrialLicenseExpiration: Trial license 1 has expired.
9	Avaya recommends that you do not enable IP Source Guard on trunk ports.
10	Avaya recommends that you do not enable Critical-IP functionality with VRRP in an SMLT environment.
11	Lossless Mode: Lossless activates in oversubscription scenarios even if rate-limiting is applied to certain ingress streams and slowing them is not necessary. Lossless gives fair access to

Item	Description
	bandwidth, meaning that if you have 3 ingress streams of 100% line rate competing on 1 egress port, lossless will slow down the sender transmit rates to a 33-33-33 percentage, and it does this by sending pause frames. If you have 2 streams coming in at 100% and a third at 20%, lossless will not interfere with this stream, the egress percentages will be 40-40-20. If the third stream transmit rate exceeds 33%, lossless will begin to apply to it as well. In this situation, if applying a meter to this stream, limiting it at under 33%, lossless doesn't activate and doesn't interfere. However, if the third stream is either broadcast or multicast traffic and a rate-limiting setting is applied instead of a meter, lossless will activate - it will send pause frames to the sender. The egress rate of the stream is not affected, it will be the one imposed by the rate-limiting setting, but the transmit rate will vary because of the pause frames.
12	Lossless Mode: In Lossless buffering mode, if you use ingress traffic with queue 1 + ingress traffic with queue 2, and the egress port is on a different asic from ingress ports, QoS queue shaper may limit the bandwidth for queue 1 under the min-rate and egress traffic may be under the expected rates.
13	ARP Table Size for ERS 5600: The maximum number of entries in the ARP table is 4096.
14	MAC Filtering List: Release 6.3 of ERS 5000 increases the maximum number of entries in the MAC Filtering List to 128. More upper limit testing is required.
15	Inexistent VLAN Mapping for MSTI: EDM/SNMP support for VLAN Mapping for MSTI is not available in Release 6.3.
16	In Release 6.3, the LLDP default settings for lldp tx-tlv and lldp tx-tlv med have been changed to enabled. In prior releases, the default setting for LLDP was disabled. These settings only apply when the switch is defaulted or the default LLDP setting is applied. When upgrading from a previous version, the configured LLDP settings will be retained.

17	You cannot enable MAC Security on LACP enabled ports. The following message displays:
	`%Cannot modify settings`
	`%MAC Security status cannot be modified. Disable LACP first.`

18	Rate Limiting: When you have the following scenario: 1. rate-limiting is performed at 10% (or by setting any percent value threshold) 2. the speed ratio between the inbound port and the client port is 10:1 (for example 10Gbps inbound link and 1Gbps client port link) 3. inbound broadcast or multicast traffic throughput on the inbound link is more than 10% link-rate speed then the client port will receive 0.1 * [inbound traffic rate] and not the expected 1Gbps broadcast or multicast traffic. Example: • inbound port link rate = 10Gbps , client outbound link rate = 1Gbps , rate limiting set to both at 10% • inbound traffic rate = 3Gbps broadcast traffic The actual client traffic received rate = 333Mbps and not the expected 1Gbps
19	In a stack configuration, SSHC configuration options are only available from the base unit

Item	Description

20	When you manually create an LLPD MED network policy, LLDP checks that the specified VLAN ID corresponds to a voice VLAN created inside the VLAN application. If the VLAN is not a voice VLAN or the VLAN does not exist, the switch displays a warning message. The switch creates the policy even if the VLAN is not voice enabled or does not exist. The switch may display one of the following messages:
	`% Policy will be set on port x with vlan-id of a non-existent vlan y`
	`% Policy will be set on port x member of the non-voice vlan y`

VLACP issue

In some situations, when you use VLACP the ERS 5000 series switches remove a link from service due to variations in the arrival time of VLACP messages (VLACP PDUs) from the far end. The issue can exist between the ERS 5600 models and ERS 8300 and ERS 8600 models when the system runs short timers with a default timeout interval of 3 time-outs or less. The ERS 5600 switches maintain a rolling history of the last 3 received VLACP PDUs (by default) and calculate the time variance across and between these VLACP messages.

SOLUTION: Increase the VLACP timeout-scale value to 3 or more.

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.

To enable some applications, for example BaySecure, Port Mirroring, and IGMP, a set number of masks and filters are required.

The following table summarizes the applications that require mask and filter resources.

Table 6: Application mask and filter resource requirements

Application	Category	Masks required	Filters required
Ethernet Routing Switch 5600 Series			
Broadcast ARP and ARP Inspection	Non QoS	1	1
DHCP Relay or DHCP Snooping	Non QoS	1	2

Application	Category	Masks required	Filters required
QoS (default untrusted policy)	QoS	2	2
QoS (DAPP with status tracking)	QoS	1	1
QoS (Auto QoS)	QoS	1	4
Port Mirroring (MAC-based)	Non QoS	1	2
EAP Authetication (EAPoL packet filter)	Non QoS	1	2
IPFIX	Non QoS	1	1
ADAC	Non QoS	1	1
RIP	Non QoS	1	1
UDP Broadcast	Non QoS	1	1
BGP (ERS 5600 only)	Non QoS	1	2
VRRP	Non QoS	1	2
OSPF	Non QoS	1	2
Content Based Forwarding (ERS 5600 only)	Non QoS	1	1
IP Source Guard	Non QoS	1	11
PIM	Non QoS	1	1

On the ERS 5600 Series switches the resources are shared across groups of ports. For each group of ports there 16 masks and 256 filers available for each mask. By default, the system consumes 2 masks and 2 filters for ARP filtering and DHCP relay on all ports, leaving 14 masks available for each group and 254 filters available for each mask and group for QoS and other non QoS applications to configure dynamically.

You can use the **`show qos diag`** command to assess the current filter resource usage for each port on ERS 5000 Series switches.

The **`show qos diag`** command displays the number of QoS masks and filters and non QoS masks and filters consumed on each port. You can determine whether an application that requires filter resources can be enabled on a port by verifying that the number of available masks and filters meets the mask and filter requirements of the application.

On the ERS 5600 Series switches, you can count the unused masks to determine the number of available masks for a port by using the output of the **`show qos diag`** command. The ERS 5600 Series switches share resources across a group of ports. The filters used by QoS or non QoS applications on a port for a specific mask determine the available filters for that mask for all ports from that group.

On the ERS 5600 Series switches, you can determine the number of 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. If the number of filters in use for a mask equals 256, you cannot use that mask on other ports from the same group.

Example - IP Source Guard on an ERS 5600 Series switch port

On ERS 5600 Series switches you need 1 mask and 11 filters to enable IP Source Guard on a port. When you view the show qos diag command output you see that port 5 is currently using a total of 4 masks. IP Source Guard uses the next available mask and, from the command output, you can see that there are 256 filters available for mask 14. So you can enable IP Source Guard.

Flow Control

The default value for flow control is asymmetric/asymm-pause-frame (forced settings / autonegotiation advertisement). When upgrading from an older software version (that had symmetic as default), the symmetric/pause-frame settings are changed to asymmetric/asymm-pause-frame.

Disabling flow control when autonegotiation is enabled:

```
ERS>enable
ERS#configure terminal
ERS(config)#interface ethernet 7-8
ERS(config-if)#auto-negotiation-advertisements port 7 1000-full
ERS(config-if)#show auto-negotiation-advertisements port 7-8
Port Autonegotiation Advertised Capabilities
---- ---------------------------------------------------------------
7                                  1000Full
8    10Full 10Half 100Full 100Half 1000Full              AsymmPause
ERS(config-if)#show interfaces 7-8
              Status          Auto                       Flow
Port Trunk Admin  Oper  Link Negotiation  Speed  Duplex Control
---- ----- ------ ----  ---- -----------  -----  ------ -------
7          Enable Up    Up   Custom       1000Mbps Full Disable
8          Enable Up    Up   Enabled      1000Mbps Full Disable
```

Enabling asymmetric flow control when autonegotiation is enabled:

```
ERS>enable
ERS#configure terminal
ERS(config)#interface ethernet 7-8
ERS(config-if)#auto-negotiation-advertisements port 7 1000-full asymm-pause-
frame
ERS(config-if)#show auto-negotiation-advertisements port 7-8
Port Autonegotiation Advertised Capabilities
---- ---------------------------------------------------------------
7                                  1000Full              AsymmPause
8    10Full 10Half 100Full 100Half 1000Full              AsymmPause
ERS(config-if)#show interfaces 7-8
              Status          Auto                       Flow
Port Trunk Admin  Oper  Link Negotiation  Speed  Duplex Control
---- ----- ------ ----  ---- -----------  -----  ------ -------
7          Enable Up    Up   Custom       1000Mbps Full Asymm
8          Enable Up    Up   Enabled      1000Mbps Full Asymm
```

Disabling flow control when autonegotiation is disabled:

```
ERS>enable
ERS#configure terminal
```

```
ERS(config)#interface ethernet 7-8
ERS(config-if)#duplex port 7-8 full
ERS(config-if)#flowcontrol port 7-8 disable
ERS(config-if)#show interfaces 7-8
              Status          Auto                       Flow
Port Trunk Admin  Oper  Link Negotiation  Speed  Duplex Control
---- ----- ------ ----  ---- -----------  -----  ------ -------
7          Enable Up    Up   Disabled     1000Mbps Full Disable
8          Enable Up    Up   Disabled     1000Mbps Full Disable
```

Enabling asymmetric flow control when autonegotiation is disabled:

```
ERS>enable
ERS#configure terminal
ERS(config)#interface ethernet 7-8
ERS(config-if)#flowcontrol port 7-8 asymmetric
ERS(config-if)#show interfaces 7-8
              Status          Auto                       Flow
Port Trunk Admin  Oper  Link Negotiation  Speed  Duplex Control
---- ----- ------ ----  ---- -----------  -----  ------ -------
7          Enable Up    Up   Disabled     1000Mbps Full Asymm
8          Enable Up    Up   Disabled     1000Mbps Full Asymm
```

Chapter 6: Fabric Attach

This chapter provides conceptual and procedural information to help you understand and configure Fabric Attach on ERS 5000 Series switches.

Related Links

Fabric Attach configuration using Enterprise Device Manager on page 74

Fabric Attach fundamentals

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

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

FA Signaling

The FA elements communicate between themselves using FA Signaling . FA Signaling is Avaya's application level protocol that leverages standard network protocols (such as LLDP, 802.1x, RADIUS, and Web Services) to exchange messages and data between FA elements to orchestrate network automation.

FA Network Elements

The FA architecture involves the following FA elements:

- FA Server–An SPB capable network device connected to the fabric edge running the FA agent in FA Server mode. FA Servers receive requests to create services with specific I-SID/VLAN bindings.
- FA Proxy–A non-SPB network device running the FA agent in FA Proxy mode. FA Proxies support I-SID/VLAN assignment definition and have the ability to advertise these assignments for possible use by an FA Server, if connectivity permits.
- FA Client–A non-SPB network attached device running the FA agent in FA Client mode and able to advertise ISID/VLAN binding requests for service creation to an FA Proxy or FA Server. Non-FA clients without an FA Agent, such as laptops, IP phones, printers or IP cameras, will also be supported in a later release.

Note:

FA Client functionality in Release 5.8 is a technology demonstration feature only.

Note:

ERS 5000 Series switches support the FA Proxy function only. The FA feature is supported in both standalone and stacked configurations.

FA Element Discovery

An FA agent which controls FA functionality resides on all FA-capable devices (FA Server, FA Proxy or FA Client). The agent executes as a normal priority task and no agent-specific configuration is necessary.

FA Proxy and FA Server elements control FA through a global FA service setting (global SPBM setting) and through per-port settings that control the transmission of FA information using FA Signaling.

The first stage of establishing FA connectivity involves element discovery. In order for FA discovery to function, FA service and per-port settings must be enabled. Once these settings are enabled, the FA agent advertises its capabilities (FA Server, FA Proxy or FA Client) through FA Signaling. Following discovery, an FA agent is aware of all FA services currently provided by the network elements to which it is directly connected. Based on this information, an FA Client agent can determine whether FA data (I-SID/VLAN assignments) should be exported to an FA Proxy that acts as an external client proxy or an FA Server.

The global FA service is always enabled. Per-port settings are, by default, enabled on FA Proxies and disabled on FA Servers.

Note:

An FA Proxy can communicate with, at most, one FA Server at a time. If multiple server connections exist, the first discovered server is considered the primary server. Multiple links (trunked) to a single server are supported as long as they form a logical interface. Multiple non-trunked links are not supported and data received on non-primary ports is ignored by an FA Proxy. FA Proxies or FA Clients can connect through a LAG/MLT to two FA Servers which form a Split-LAG or SMLT pair. Connections which may create loops, to multiple servers that are not in Split-LAG or SMLT mode, are not supported.

An FA Server can communicate with multiple, different FA Proxies and FA Clients.

FA agent startup and initialization

During the FA agent startup and initialization sequence, the following are restored from non-volatile memory:

- FA service status
- FA port-level settings

- Auto Attach status
- FA Proxy status
- message authentication requirements
- previously configured I-SID/VLAN assignments

In a stack environment, FA agent startup and initialization occurs on every unit in the stack, using the data restored from non-volatile memory.

The initialization sequence can also include operations geared towards cleaning-up settings that were previously configured in support of FA I-SID/VLAN assignments that were active on an FA proxy or an FA server before a system reset.

FA LLDP extensions

The Fabric Attach (FA) TLVs described in this section are implemented as extensions to the LLPD standard, using the flexible extension mechanism supported by the standard. These TLVs use TLV type 127 as described in the 802.1ab (LLDP) standard.

Avaya Fabric Attach Element TLV

With the Avaya FA Element TLV, FA elements advertise their FA capabilities. This data forms the basis for FA element discovery and determines the state machine used by FA entities. This information is received, processed and stored by the receiving switch so that it is immediately accessible for internal applications.

The Organizationally Specific Avaya FA Element TLV contains the following data:

- FA Element Type – indicates element capabilities
- FA Element Management VLAN – identifies the management VLAN
- FA Element System ID - unique system identifier used to support element discovery and tracking.

The FA Element TLV is included in all LLDPDUs when the FA service is enabled and when the port-level transmission flags associated with this TLV are enabled. Port-level settings can be configured with LLDP support, using the **`lldp tx-tlv vendor avaya`** ACLI command, and with FA support, using the **`fa port-enable`** ACLI command.

With the FA service enabled, LLDPDUs containing proprietary Avaya TLVs are transmitted on links that may or may not have Avaya components at the far end. Since the LLDP standard dictates that unrecognized but well-formed TLVs in received LLDPDUs should be ignored, this should not cause any issues.

This behavior is different from the way other proprietary Avaya LLDP TLVs are handled. The other proprietary Avaya TLVs are only included in LLDPUs generated on links that have recognized Avaya elements, specifically Avaya telephony gear, at the far end.

Avaya FA I-SID-to-VLAN Assignment TLV

With the Avaya FA I-SID-to-VLAN Assignment TLV, an FA Proxy or FA Client distributes I-SID-to-VLAN assignments to the FA Server. This information is received, processed and stored by the receiving switch so that it is immediately accessible for internal applications.

I-SID/VLAN Assignment TLV data integrity and source validation is supported through the use of the HMAC-SHA256 message authentication algorithm.

I-SID-to-VLAN assignment requests can be accepted (active) or rejected by an FA Server.

The FA I-SID-to-VLAN Assignment TLV is only included in a LLDPDU when complementary FA element (FA Proxy, FA Server, or FA Client) end devices are directly connected. The associated port-level transmit flags must be enabled, as well.

The Organizationally Specific Avaya FA I-SID-to-VLAN Assignment TLV contains the following data:

- VLAN ID – identifies the VLAN component of the I-SID-to-VLAN mapping
- I-SID – identifies the I-SID component of the I-SID-to-VLAN mapping
- Status–contains information related to the processing of the I-SID-to-VLAN mapping

Multiple I-SID-to-VLAN assignments may be included in a single TLV.

All I-SID-to-VLAN assignments defined on an FA Proxy, as well as those received from FA Clients when FA Proxy external client proxy support is enabled, start in the 'pending' state. This state is updated based on feedback received from the FA Server. If an assignment is accepted by the FA Server, its state is updated to 'active'. A server may also reject proposed I-SID-to-VLAN assignments. In this case, the assignment state is updated to 'rejected'.

Avaya TLV Transmit Flags

With the transmit flags, you can choose on a port-level basis, which LLDP TLVs (including the Avaya TLV such as Call Server TLV or FA TLVs) to include in transmitted LLDPDUs, and which to exclude. These flags are independent of the configured TLV data. Therefore, even if data for a specific TLV is configured, the TLV is only included in LLDPDUs on ports for which the TLV is enabled for transmission.

By default, the transmit flags are set to *enabled* for all of the Avaya TLVs on all ports. The transmit status for the PoE Conservation Levels TLV default depends on the PoE support for the device. The transmit flags for the new FA TLVs are set to *enabled* by default on FA Proxies and *disabled* on FA Servers, on all ports. The transmit flag values for the FA TLVs can also be manipulated through the FA support, with the **`fa port-enable`** ACLI command.

FA proxy I-SID-to-VLAN assignment

Although administrators typically configure I-SID-to-VLAN bindings on FA proxies, I-SID-to-VLAN bindings can also be received by FA Proxies from FA Clients. If external client proxy support is enabled, standard processing requirements for bindings received from an FA Client are managed the same way that processing requirements for locally configured bindings are managed.

Each configured I-SID-to-VLAN association creates a C-VLAN User Network Interface (UNI), when the assignment is active, and accepted by an FA Server.

Note:

ERS 5000 Series switches, with FA enabled, support only C-VLAN UNIs and do not support switched UNIs.

If an I-SID-to-VLAN assignment is accepted by the FA Server, the assignment state is updated to *active*. If an I-SID-to-VLAN assignment is not accepted by the FA Server, the assignment state is updated to *rejected*.

The FA Proxy receives and displays assignment status information from the FA Server for each pending I-SID-to-VLAN assignment. Possible responses include:

- Assignment accepted (2)
- Rejection: generic (3)
- Rejection: Fabric Attach resources unavailable (4)
- Rejection: VLAN invalid (6)
- Rejection: VLAN resources unavailable (8)
- Rejection: application interaction issue (9)

Note:

Data exchanges (I-SID/VLAN assignments) between an FA Proxy and an FA Server/FA Client are supported, as are exchanges between an FA Server and an FA Proxy/FA Client. FA Proxy to FAProxy and FA Server to FA Server interactions are not supported.

ERS 5000 series switches support the exchange of I-SID-to-VLAN assignment information from an FA proxy to an FA server and FA client. The exchange of I-SID-to-VLAN assignment information from an FA server to an FA proxy and FA client is also supported.

FA data processing

Following discovery, an FA Proxy or FA Client transmits locally-defined I-SID/VLAN assignments through FA Signaling to an FA Server, which accepts or rejects these assignments.

The I-SID/VLAN assignment acceptance by the server can require actions to be performed by the FA agent on both the FA Proxy and the FA Server, to appropriately configure the communication channel (uplink) between the FA Proxy or FA Client and FA Server. Most actions undertaken based on assignment acceptance are undone when the I-SID/VLAN assignment is no longer needed.

I-SID/VLAN assignment rejection by the FA Server requires the FA Proxy to clean up any settings that the FA agent made related to feature operation, as well as log the rejection (and any associated error type information) for later analysis by an administrator. The amount of clean-up required depends on whether the port VLAN membership was established by the FA Proxy agent or by the administrator outside of the FA feature operation. Specifically, an uplink port associated with a VLAN because of an accepted FA Proxy I-SID/VLAN assignment (and not because of an explicit administrator port VLAN membership action) clear the port VLAN membership when the related I-SID/VLAN assignment is rejected by the FA Server or deleted by the FA Proxy administrator. Once the FA agent establishes the port tagging status, it remains in effect regardless of I-SID/VLAN assignment status.

VLANs that are automatically created on an FA Proxy due to I-SID/VLAN assignment acceptance are automatically deleted when bindings are rejected or deleted.

No more than a single log message is generated for a rejected I-SID/VLAN assignment, regardless of how many times the assignments have been requested and rejected. Assignments that are rejected, accepted, and later rejected result in a log message being generated for each “new” rejection (two I-SID/VLAN assignment rejection log messages are generated in this case).

FA Proxy I-SID/VLAN assignment addition actions:

- Create port-based VLAN corresponding to I-SID/VLAN assignment VLAN.
- Update port VLAN membership to include I-SID/VLAN assignment VLAN.
- Update port VLAN tagging status to ensure egress traffic is tagged.

FA Server I-SID/VLAN assignment addition actions:

- Create SPBM switched UNI VLAN corresponding to I-SID/VLAN assignment VLAN.
- Update downlink port VLAN tagging status to ensure egress traffic is tagged. Tagging status for FA client connections is determined by the client type.
- Update I-SID/VLAN mapping data to ensure Shortest Path Bridging-MAC (SPBM)-switched UNI support is enabled for the I-SID/VLAN/port tuple (in other words, create switched UNI). Port VLAN membership is updated by this action.
- Update downlink port VLAN ID (PVID) for untagged client connections (if a valid default VLAN in the range of 1-4094 was specified by the client and if the VLAN in the binding being activated equals the specified default VLAN).

Additional actions can be required for I-SID/VLAN binding state transitions involving FA Client-generated data. The communication channel (that is, the downlink) between the FA Client and FA Proxy must be appropriately configured. This can require actions to be performed on the switch.

FA Proxy external client proxy I-SID/VLAN assignment addition actions:

- Update downlink port VLAN membership to include I-SID/VLAN assignment VLAN.
- Update downlink port VLAN tagging status based on the FA Client type (tagged – ‘tagAll’/ untagged – ‘untagPvidOnly’).
- Update downlink port VLAN ID (PVID) for untagged FA Clients (if a valid default VLAN [1..4094] was specified by the client and if the VLAN in the binding being activated equals the specified default VLAN).

Each of these actions is performed by the FA Proxy and FA Server for each I-SID/VLAN assignment, unless the required data/settings have already been configured by the administrator. The successful transition from ‘pending’ to ‘active’ is gated by the successful completion of these actions. The FA agent tracks which settings have been updated based on I-SID/VLAN assignment processing (comparing them with settings established by the administrator), and cleans-up or undoes the settings that are related to I-SID/VLAN assignment support as much as possible when an assignment is no longer needed.

I-SID/VLAN assignment state transitions from ‘active’ to ‘rejected’ require complementary actions be performed by the FA Proxy and the FA Server to eliminate assignment-related settings:

FA Proxy I-SID/VLAN assignment deletion actions:

- Update port VLAN membership to exclude I-SID/VLAN assignment VLAN.

Note:

The FA Proxy deletes port-based VLANs created during binding activation if the VLAN is not associated with other ports.

FA Server I-SID/VLAN assignment deletion actions:

- Delete I-SID/VLAN/port association data to disable SPBM-switched UNI support for the I- SID/ VLAN/port tuple (to delete switched UNI). This action updates port VLAN membership.
- Delete SPBM-switched UNI VLAN corresponding to I-SID/VLAN assignment VLAN.
- Default downlink port VLAN ID (PVID) for untagged clients. Downlink port VLAN tagging status remains unchanged.

State transitions related to FA Client-generated bindings require additional complementary actions to be performed by the FA Proxy to eliminate assignment-related settings:

FA Proxy external client proxy I-SID/VLAN assignment deletion actions:

- Update downlink port VLAN membership to exclude I-SID/VLAN assignment VLAN.
- Default downlink port VLAN ID (PVID) for untagged clients.

Note:

The FA Proxy deletes port-based VLANs created during binding activation if the VLAN is not associated with other ports.

Assignment status data returned by the FA Server for each pending I-SID/VLAN assignment drives the FA Proxy response processing. Assignment rejections can include information to indicate the reason for the rejection.

Rejection error codes include:

- FA resources unavailable(4)–the resources that are required for the FA agent to support additional I-SID/VLAN assignments are currently exhausted. The maximum number of assignments that can be supported has been reached.
- VLAN invalid(6)–the specified VLAN can’t be used to create a switched UNI at this time. The VLAN already exists and is either inactive or has an incorrect type for this application.
- VLAN resources unavailable(8)–the maximum number of VLANs that can be supported by the device has been reached.
- Application interaction issue(9)–a failure has been detected during FA interactions with the VLAN and/or the SPBM applications. The VLAN operations to create the required SPBM switched UNI VLAN or enable port tagging may have failed or the SPBM operation to create the switched UNI may have failed.

As with the actions initiated to support an assignment addition, actions related to assignment deletion are performed only if the targeted data was created during the I-SID/VLAN assignment addition phase. Previously-existing configuration data is not changed. No artifacts are left behind to indicate that automated operations have taken place, following an addition or deletion sequence. This goal may not always be achievable but all attempts are made to satisfy this requirement.

In addition to explicit I-SID/VLAN assignment state transitions, several events can occur that initiate assignment deletion processing. These include:

- I-SID/VLAN assignment timeout–A “last updated” timestamp is associated with all active assignments on the FA Server. When this value is not updated for a pre-determined amount of time, the I-SID/VLAN assignment is considered obsolete. Obsolete assignment data and related settings are removed by the FA server agent. The timeout duration value allows FA Server settings to be maintained if temporary connectivity issues are encountered.

  I-SID/VLAN binding timeout is also performed by an FA Proxy when it is providing client proxy services and FA Client data is present. Processing similar to that performed by the FA Server related to data aging is supported.
- I-SID/VLAN assignment list updates–The current I-SID/VLAN assignment list is advertised by an FA Proxy at regular intervals (dictated by FA Signaling). During processing of this data, an FA Server must handle list updates and delete assignments from previous advertisements that are no longer present. Though these entries would be processed appropriately when they timeout, the FA agent attempts to update the data in real-time and initiates deletion immediately upon detection of this condition.
- FA Server inactivity timeout–If primary FA Server advertisements are not received for a pre-determined amount of time, the I-SID/VLAN assignments accepted by the server are considered rejected. I-SID/VLAN assignment data is defaulted (reverts to the ‘pending’ state) and related settings are removed by the FA Proxy agent. The timeout duration value has been chosen to allow FA Proxy settings to be maintained if temporary connectivity issues are encountered.

FA Proxy and FA Server connection maintenance

An FA Proxy can only interact with one FA Server at a time. If multiple server connections exist, the first discovered server is considered the primary server. All other servers discovered after this point in time are considered alternates. Typically only a single FA Server is discovered. If multiple servers are discovered, an indication is logged to identify this situation in case it is not intended. I-SID/VLAN assignment data is only exchanged between the FA Proxy and the primary FA Server.

Primary server failure is detected using a capabilities advertisement timeout. Once a predefined period of time without an FA Server Signaling from the current primary server expires, the primary server becomes undefined. Any FA Proxy I-SID/VLAN assignments previously accepted by the server are defaulted (reset to the ‘pending’ state) and related settings are cleared. An informational message (primary server lost) is logged when this transition occurs. I-SID/VLAN assignment data is not advertised until a new primary FA Server is selected. The same algorithm used at startup to select an initial primary server is used to select a new primary server.

FA Proxy/FA Server connectivity using Multi-link Trunking (MLT), Distributed Multi-Link Trunking (DMLT) or Split Multi-Link Trunking (SMLT) connections is supported.

Multiple connections to the same FA server are treated as a single logical connection by the FA Proxy. The FA agent reconciles any issues related to MLT, DMLT and SMLT server connectivity and recognizes server uniqueness in the presence of (potentially) multiple capabilities advertisements (that is, FA Signaling received on multiple ports generated by the same server).

In MLT, DMLT and SMLT environments, FA Signaling is generated and received on all links connecting the FA Proxy and FA Server. An FA Proxy receiving an FA Server advertisement determines if a primary FA Server has been selected. If not, the FA Element System ID associated with an advertising FA Server is saved and primary server selection is completed. Once a primary server has been selected, system ID data associated with FA Server advertisements received on other ports is compared against the primary server data. If the system ID values are not the same, an error indication is logged. In all cases, the FA Proxy only generates FA Signaling containing I-SID/VLAN assignment data on the interfaces associated with the primary FA Server.

Note:

The FA Element System ID is structured such that the same system ID is generated on all links associated with a trunk connection between an FA Proxy and an FA Server even in an SMLT scenario where different physical devices are acting as a single logical entity.

In an SMLT environment, an FA Server takes additional actions to ensure that data is synchronized on both SMLT aggregation peers. In this configuration, the FA Server that receives and accepts advertised FA I-SID/VLAN assignments is responsible for generating messages that are sent across the Inter-Switch Trunk (IST) to inform the partner aggregation switch about FA settings that have been configured (for example, SPBM switched UNI VLAN). Similar actions are required when I-SID/VLAN assignments are deactivated.

Agent Stacking functionality

The FA agent is able to function in both standalone and stacked configurations. In a stack, the base unit FA agent acts as the master and pushes its configuration settings to all non-base units (NBUs), to synchronize data across all units. FA agents are active on all units and are able to process stack events as well as data distribution messages.

On an FA Proxy, connections to the primary FA Server can exist on any unit in the stack. When the unit with the active FA Proxy-to-FA primary server interface leaves the stack, any I-SID-to-VLAN assignments accepted by the server are immediately aged-out. I-SID-to-VLAN assignment data is restored to the default *pending* state and related settings are removed by the FA Proxy agent.

FA message authentication and integrity protection

In order to secure the FA communication in terms of data integrity and authenticity, a keyed-hash message authentication code transmitted with the I-SID/VLAN assignment data can be used to protect the FA Proxy/FA Server I-SID/VLAN assignment exchanges. The standard HMAC-SHA256 algorithm is used to calculate the message authentication code (digest) involving a cryptographic hash function (SHA-256) in combination with a shared secret key. The key is symmetric (known by both source and destination parties). By default, FA message authentication is enabled and a default key is defined to provide secure communication out-of-the-box.

On secure (SSH) images, you can enable or disable FA message authentication. On non-secure images, message authentication cannot be enabled.

When FA message authentication is enabled, the FA key (default or configured) is used to generate a Hash-based Message Authentication Code (HMAC) digest that is included in FA I-SID/VLAN Assignment TLVs. Upon receipt, the HMAC digest is recomputed for the TLV data and compared against the digest included in the TLV. If the digests are the same, the data is valid. If not, the data is considered invalid and is ignored.

The FA secure communication setting (enabled/disabled) and the symmetric key data are maintained across resets and restored during FA initialization.

Auto Attach

FA devices can use Auto Attach to extract management VLAN data from the primary FA server advertisements. FA devices uses the FA server advertisement data to update the in-use management VLAN and initiate IP address acquisition using DHCP.

Although the Auto Attach and FA operations are closely associated, you can enable or disable Auto Attach separately from FA, on an FA Proxy or FA Server. The Auto Attach feature is dependant on data that is only available during exchanges between the FA Proxy and the FA Server, specifically, after a primary FA Server is selected. Auto Attach must be enabled on the FA Server or FA Proxy before management VLAN information is included in the generated FA Element TLV. Auto Attach is enabled by default on FA Proxies and disabled by default on FA Servers.

When an FA Proxy, with Auto Attach enabled, receives the FA Element TLV, the switch compares received management VLAN information with information about the currently configured management VLAN. If the management VLAN information does not match, the FA Proxy initiates the following:

- VLAN creation — If the FA Server-specified management VLAN does not exist on the FA Proxy, Auto Attach creates a port-based VLAN.
- Management VLAN — The created port-based VLAN becomes the designated management VLAN for the FA Proxy. No operations related to the previous management VLAN, such as port membership updates or VLAN deletion, are performed.
- Port VLAN membership — Auto Attach updates the port VLAN membership to ensure that the uplink port through which the primary FA Server is accessed is a member of the management VLAN for network accessibility. Auto Attach also updates the port VLAN membership to ensure that the downlink port through which the FA Proxy, or FA Client is accessed is a member of the management VLAN.
- IP address acquisition — Auto Attach initiates IP address acquisition through DHCP if an IP address was not already manually configured. This operation is equivalent to using the dhcp-when-needed parameter with the **`ip address source`** command. For more information, see *Obtaining an in-band management IP address automatically*, in *Getting Started with Avaya Ethernet Routing Switch 5000 Series*, NN47200–303.

If Auto Attach is not enabled on the FA Proxy, or if the VLAN ID for the management VLAN is not in the range of 1 to 4094, the switch does not perform any Auto Attach-specific functions.

Note:

The FA Proxy does not update the acquired management VLAN, or IP address information if connection with the primary FA Server is lost. The management VLAN or IP information is updated when the management VLAN advertised by the current primary FA Server changes, or if another primary FA Server is selected, and advertises new management VLAN data.

Management VLAN and port membership updates performed by Auto Attach are maintained in non-volatile memory and are restored following a system reset. The network administrator can delete or update this information as required.

FA Clients

ERS 5000 Series switches cannot function as FA clients, but switches configured as FA Proxies can help extend the fabric edge by connecting to other devices that are configured as FA Clients.

FA Clients connect to an FA Proxy through standard, non MAC-in-MAC access ports, advertising configured I-SID/VLAN requests to the FA Server. In this scenario, the FA Proxy acts as a client proxy for the FA Client by passing I-SID/VLAN binding requests to a discovered FA Server and returning assignment status information to the FA Client. FA Clients may connect directly to an FA Server as well.

Note:

External client proxy support must be enabled on an FA Proxy switch before FA client data is accepted by the FA Proxy. By default, external client proxy support is enabled on an FA Proxy.

I-SID/VLAN bindings received from an FA Client by an FA Proxy acting as a proxy for external clients are processed in much the same way locally administered assignments are processed. FA Proxy response processing takes care of VLAN creation and updates VLAN membership and tagging of the FA Server uplink port if necessary.

If the I-SID/VLAN client assignment is rejected by the FA Server, the FA Proxy performs any required clean-up tasks and also logs the rejection and any associated error type information for later analysis by an administrator.

Note:

FA Clients are not available yet at the time of the development of this document. The above description of the FA Clients is made for clarity of the Avaya Fabric Attach architecture.

Fabric Attach configuration using the Avaya Command Line Interface

This section provides procedural information you can use to configure Fabric Attach (FA) using the Avaya Command Line Interface (ACLI).

Displaying FA-specific settings

Use this procedure to display the FA configuration status for an FA Proxy.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. To display the FA configuration status, enter the following command:

   ```
   show fa spbm
   ```

Example

This example shows sample output for the **`show fa spbm`** command.

```
5650TD-PWR#show fa spbm

Fabric Attach Service Status: Enabled
Fabric Attach Element Type: Proxy
Fabric Attach Auto Attach Status: Enabled
Fabric Attach Message Authentication Status: Disabled
Fabric Attach Proxy Status: Enabled
Fabric Attach Primary Server Id: <none>
Fabric Attach Primary Server Descr: <none>

5650TD-PWR#
```

Configuring FA Proxy external client proxy support

Use this procedure to enable or disable FA Proxy external client proxy support.

About this task

This operation enables or disables FA Proxy external client proxy support. It does not impact communication with an FA Server.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To enable FA Proxy external client proxy support, enter either of the following commands:

   ```
   fa proxy
   ```

   OR

   ```
   default fa proxy
   ```

3. To disable FA Proxy external client proxy support, enter the following command:

   ```
   no fa proxy
   ```

Creating an I-SID-to-VLAN assignment on an FA proxy

About this task

Use this procedure to create an association between an SPBM Service Instance Identifier (I-SID) and a VLAN on an FA Proxy.

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. To create an I-SID-to-VLAN assignment, enter the following command:

   `i-sid <1-16777214> vlan <1-4094>`

Result

Each FA Proxy I-SID-to-VLAN assignment creates a C-VLAN User Network Interface (UNI) when the assignment is active, and accepted by an FA server.

Example

This example shows a sample command for creating an association between I-SID 600 and VLAN 3

```
5650TD-PWR+(config)#i-sid 600 vlan 3
5650TD-PWR+(config)#
```

Variable definitions

The following table describes the parameters for the **`i-sid <1-16777214> vlan <1-4094>`** command

Variable	Value
i-sid *<1-16777214>*	Specifies the I-SID to associate with the selected VLAN. Values range from 1 to 16777214.
vlan *<1-4094>*	Specifies the VLAN to associate with the selected I-SID. Values range from 1 to 4094.

Deleting an I-SID-to-VLAN assignment on an FA Proxy

Use this procedure to remove the association between an I-SID and a VLAN on an FA Proxy.

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. To remove a specific I-SID-to-VLAN assignment, enter the following command:

   ```
   no i-sid <I-SID> vlan <VLAN>
   ```

3. To remove all configured I-SID-to-VLAN assignments, enter the following command:

   ```
   default i-sid
   ```

Variable definitions

The following table describes the parameters for the **`no i-sid <I-SID> vlan <VLAN>`** command

Variable	Value
i-sid *<1-16777214>*	Specifies the I-SID of the specific I-SID-to-VLAN assignment to remove. Values range from 1 to 16777214.
vlan *<1-4094>*	Specifies the VLAN of the specific I-SID-to-VLAN assignment to remove. Values range from 1 to 4094.

Displaying I-SID-to-VLAN assignment information

Use this procedure to display information about I-SID-to-VLAN assignments configured on an FA Proxy.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. To display I-SID-to-VLAN assignment information, enter the following command:

   ```
   show fa i-sid [<1-16777214>]
   ```

Variable definitions

The following table describes the parameters for the **`show fa i-sid [<1-16777214>]`** command

Variable	Value
[<1-16777214>]	Specifies the Fabric Attach I-SID for which to display I-SID-to-VLAN assignment information. Values range from 1 to 16777214. If you do not specify a I-SID value, the switch displays information for all configured I-SID-to-VLAN assignments.

Displaying I-SID-to-VLAN assignment C-VLAN UNI information

Use this procedure to display information about C-VLAN UNIs created with I-SID-to-VLAN assignments configured on an FA Proxy.

About this task

Each FA Proxy I-SID-to-VLAN assignment creates a C-VLAN UNI when the assignment is active, and accepted by an FA Server.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. To display C-VLAN UNI information, enter the following command:

   ```
   show i-sid [<1-16777214>]
   ```

Example

This example shows sample C-VLAN UNI information for the I-SID 500-to-VLAN 5 assignment, using the **`show i-sid [<1-16777214>]`** command:

```
5650TD-PWR>show i-sid 500
I-SID     Vid  UNI-type    Ports
--------- ---- ----------- ------------
500       5    C-VLAN      2/91
```

This example shows sample C-VLAN UNI information for all I-SID-to-VLAN assignments configured on the switch, using the **`show i-sid`** command:

```
5650TD-PWR>show i-sid
I-SID     Vid  UNI-type    Ports
--------- ---- ----------- ------------
500       5    C-VLAN      2/91
600       6    C-VLAN      2/91,3/1
13849     138  C-VLAN      2/91
16000000  1000 C-VLAN      2/91
```

Variable definitions

The following table describes the parameters for the **`show i-sid [<1-16777214>]`** command

Variable	Value
[<1-16777214>]	Specifies the I-SID of the specific I-SID-to-VLAN for which to display UNI information. Values range from 1 to 16777214. If you do not specify a I-SID value, the switch displays UNI information for all configured I-SID-to-VLAN assignments.

Configuring FA on switch ports

Use this procedure to enable or disable the FA operation on one or more switch ports.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To configure the FA operation on switch ports, enter the following command:

```
[no][default] fa port-enable [<portlist>]
```

Variable definitions

The following table describes the parameters for the `[no][default] fa port-enable [<portlist>]` command.

Variable	Value
[<portlist>]	Enables the FA operation on the specified switch port or ports. If you do not specify a port, the FA operation is enabled on all switch ports.
[no]	Disables the FA operation on the specified switch port or ports. If you do not specify a port or ports, the FA operation is disabled on all switch ports.
[default]	Restores the FA operation on all switch ports to default. Default: Enabled

Displaying switch port FA operation status

Use this procedure to display if FA is enabled or disabled on one or more switch ports.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. To display FA configuration information, enter the following command:

   ```
   show fa port-enable [<portlist>]
   ```

Variable definitions

The following table describes the parameters for the `show fa port-enable [<portlist>]` command.

Variable	Value
[<portlist>]	Specifies the switch port or ports for which to display Fabric Attach configuration information. If you do not specify a port or ports, the switch displays Fabric Attach information for all switch ports.

Configuring Auto Attach support

Use the following procedure to enable or disable Auto Attach on an FA Proxy.

About this task

When Auto Attach is enabled on an FA Proxy, the switch extracts management VLAN data from the primary FA server.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To enable Auto Attach, enter either of the following commands:

   ```
   fa auto-attach
   ```

   OR

   ```
   default fa auto-attach
   ```

3. To disable Auto Attach, enter the following command:

   ```
   no fa auto-attach
   ```

Fabric Attach configuration using Enterprise Device Manager

Use the procedures in this section to configure Fabric Attach (FA) using Enterprise Device Manager.

Related Links

Fabric Attach on page 58
Configuring Fabric Attach on page 74
Displaying FA-specific settings on page 75
Creating an I-SID/VLAN assignment on an FA Proxy on page 76
Deleting an I-SID/VLAN assignment on an FA Proxy on page 77
Configuring per-port FA settings on page 77

Configuring Fabric Attach

Procedure

1. From the navigation tree, select **Edit > Fabric Attach**.
2. Click the **SPBM** tab.
3. To enable or disable Auto Attach support, click **enable** or **disable** in the **AutoAttachService** field.

4. To enable or disable Message authentication support, click **enable** or **disable** in the **MsgAuthStatus** field.
5. Enter the desired password for message authentication in the **MsgAuthKey** field.
6. Confirm the password for message authentication in the **Confirm MsgAuthKey** field.
7. To enable or disable Fabric Attach external client proxy support, click **enable** or **disable** in the **HostProxyStatus** field.
8. Click **Apply**.

Related Links

Fabric Attach configuration using Enterprise Device Manager on page 74

Variable definitions on page 75

Variable definitions

Use the data in the following table to use the **SPBM** tab.

Variable	Value
Service	Displays the service status.
Element Type	Indicates whether the switch functions as an FA Proxy or FA Server.
PrimaryServerId	Displays the ID of the primary server.
PrimaryServerDescr	Displays the FA Server description.
AutoAttachService	Specifies whether the Auto Attach support is enabled or disabled.
MsgAuthStatus	Specifies whether the message authentication support is enabled or disabled.
MsgAuthKey	Specifies the password for message authentication.
Confirm MsgAuthKey	Requires entering again the password for message authentication.
HostProxyStatus	Specifies whether the external client proxy support is enabled or disabled.

Related Links

Configuring Fabric Attach on page 74

Displaying FA-specific settings

Use the following procedure to view FA-specific settings:

Procedure

1. In the navigation tree, expand the following folders: **Configuration>Edit**.
2. Click **Fabric Attach**.

3. In the work area, click the **I-SID** tab.

Related Links

Fabric Attach configuration using Enterprise Device Manager on page 74
Variable Definitions on page 76

Variable Definitions

Variable	Value
Isid	Indicates the I-SID for this I-SID/VLAN assignment.
Vlan	Indicates the VLAN for this I-SID/VLAN assignment.
State	Indicates the assignment state.

Related Links

Displaying FA-specific settings on page 75

Creating an I-SID/VLAN assignment on an FA Proxy

Use the following procedure to create an I-SID/VLAN assignment on an FA Proxy.

Procedure

1. In the navigation tree, expand the following folders: **Configuration>Edit**.
2. Click **Fabric Attach**.
3. In the work area, click the **I-SID** tab.
4. Click **Insert**.
5. Specify an I-SID in the **Isid** field.
6. Specify a VLAN in the **Vlan** field.
7. Click **Insert**.

Related Links

Fabric Attach configuration using Enterprise Device Manager on page 74
Variable definitions on page 76

Variable definitions

Use the data in the following table to use the **I-SID** tab.

Name	Description
Isid	Specifies the I-SID to associate with a VLAN.
Vlan	Specifies the VLAN to associate with an I-SID.

Related Links

Creating an I-SID/VLAN assignment on an FA Proxy on page 76

Deleting an I-SID/VLAN assignment on an FA Proxy

Use the following procedure to delete an I-SID/VLAN assignment on an FA Proxy.

Procedure

1. In the navigation tree, expand the following folders: **Configuration>Edit**.
2. Click **Fabric Attach**.
3. In the work area, click the **I-SID** tab.
4. Select an I-SID/VLAN assignment.
5. Click **Delete**.
6. Click **Yes**.

Related Links

Fabric Attach configuration using Enterprise Device Manager on page 74

Configuring per-port FA settings

Use the following procedure to determine whether FA data is included in FA Signaling.

Procedure

1. From the navigation tree, select **Edit**.
2. In the Edit tree, double-click **Fabric Attach**.
3. On the work area, click the **Ports** tab.
4. To enable or disable the transmission of FA information in FA Signaling, select **enabled** or **disabled** in the **State** field for a specific port or ports.
5. Click **Apply**.

Related Links

Fabric Attach configuration using Enterprise Device Manager on page 74

Variable Definition on page 77

Variable Definition

Variable	Value
IfIndex	Specifies the interface for which to enable or disable FA operation.
State	Indicates whether FA operation is enabled or disabled.
enabled	Indicates that FA operation is enabled on corresponding interfaces.

Variable	Value
disabled	Indicates that FA operation is disabled on corresponding interfaces.

Related Links

Configuring per-port FA settings on page 77