Avaya Release Notes — Release 5.6 Avaya Ethernet Routing Switch 4000 Series

Release 5.6
NN47205-400
Issue 08.04
May 2013

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

Licence types

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

Heritage Nortel Software

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

Copyright

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

Third Party Components

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

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your

Avaya Toll Fraud intervention

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

Trademarks

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

This document describes new features, hardware, upgrade alerts, known and resolved issues, and limitations for Avaya Ethernet Routing Switch 4000 Series, Software Release 5.6.

For information on how you can obtain and use the embedded version of Enterprise Device Manager (EDM), see *Avaya Ethernet Routing Switch 4000 Series Fundamentals*, (NN47205-102). An off-box version of EDM is also available as a free, downloadable software plug-in installed on Configuration and Orchestration Manager (COM), purchased separately. For more information about COM, see www.avaya.com/support.

The Avaya Ethernet Routing Switch 4000 Series, supported by software release 5.6, includes the following switch models:

- Avaya Ethernet Routing Switch 4524GT
- Avaya Ethernet Routing Switch 4524GT-PWR
- Avaya Ethernet Routing Switch 4526FX
- Avaya Ethernet Routing Switch 4526GTX
- Avaya Ethernet Routing Switch 4526GTX -PWR
- Avaya Ethernet Routing Switch 4526T
- Avaya Ethernet Routing Switch 4526T-PWR
- Avaya Ethernet Routing Switch 4548GT
- Avaya Ethernet Routing Switch 4548GT-PWR
- Avaya Ethernet Routing Switch 4550T
- Avaya Ethernet Routing Switch 4550T-PWR
- Avaya Ethernet Routing Switch 4550T-PWR+
- Avaya Ethernet Routing Switch 4526T-PWR+
- Avaya Ethernet Routing Switch 4850GTS
- Avaya Ethernet Routing Switch 4850GTS-PWR+
- Avaya Ethernet Routing Switch 4826GTS
- Avaya Ethernet Routing Switch 4826GTS-PWR+

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. One of the benefits of operating Avaya Ethernet Routing Switch 4000 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.

These Release Notes provide the latest information about Software Release 5.6, as well as operational issues not included in the documentation suite.

For a complete list of documentation in the 4000 Series suite, see *Avaya Ethernet Routing Switch 4000 Series Documentation Road Map,* (NN47205-101) .

The information in these Release Notes supersedes applicable information in other documentation.

Chapter 2: New in this release

The following sections detail what is new in Avaya Ethernet Routing Switch 4000 Series Release Notes — Software Release 5.6.

Features

See the following sections for information about new features.

Disable MAC Learning

You can use Disable MAC Learning on a port when you want to control how the switch manages the Layer 2 Forwarding Database (FDB) entries. Disabling MAC learning can be used to prevent MAC tables from filling unnecessarily. You can use Disable MAC Learning in combination with Static MAC FDB Entry.

Enterprise Device Manager (EDM) Enhancements

Release 5.6 includes the following EDM user interface enhancements:

- a Save Config button was added to the Navigation tree toolbar to allow you to quickly and easily save a configuration.
- a search function, called Auto Complete Search, appears just beneath the Navigation tree toolbar. You can use the entry field in this search function to help you find navigation tree folders quickly. For example, you can enter “IP” in the search window and the navigation tree changes to reveal only items related to the text “IP”.
- for tabs that display a table, there are new buttons in the toolbar, the Copy/Paste/Undo and Print buttons that allow you to copy and paste (and undo) cell data between rows for the same column or field. The Print button allows you to print the contents of the table.

Equal Cost MultiPath (ECMP)

Equal Cost MultiPath (ECMP) allows routers to use up to four equal cost paths to the same destination prefix thereby improving resiliency and network utilization. The multiple paths can be used for load sharing of traffic and allow faster convergence to other active paths in case of network failure. By maximizing load sharing among equal cost paths, the switch can use the links between routers more efficiently when sending IP traffic.

Industry Standard CLI Improvements

In Release 5.6 selected ACLI commands for ARP, Spanning Tree, and VLAN have been modified to a CLI syntax which more closely matches that of industry standard implementations. The interface retains backwards compatibility; previous command and ASCII configuration files you created prior to Release 5.6 will function normally. When running Release 5.6 or later software, the new command syntax displays by default in any CLI show or output.

Internet Group Management Protocol (IGMP) Querier

IGMP Querier provides a means to generate IGMP queries to designated sources when the switch or VLANs are operating in Layer 2 mode (that is, without the need of a local IP Multicast router). IGMP Querier sends IGMP general queries to all ports, Multi-Link Trunks (MLT), Distributed Multi-Link Trunks (DMLT), and Link Aggregation Groups (LAG) on the configured VLAN.

Internet Group Management Protocol (IGMP) version 3 Snooping and Proxy

From Release 5.6 and up the switch supports full IGMPv3 Snooping and Proxy. IGMPv3 Snooping provides the ability to pack multiple group members in a single report message to reduce the amount of network traffic. When you enable IGMPv3 Snooping, you can use IGMP proxy to receive and consolidate multiple reports for the same multicast group. Additionally, IGMP selective channel blocking has been implemented to allow control of the IGMP join processing on any given port.

IP Phone Automatic PoE Changes

PoE settings and IP Phone discovery have been enhanced to allow the provision of PoE priority levels and power limits when the system discovers an IP Phone.

Layer 3 Brouter Port

From Release 5.6 and up, the switch supports the configuration of brouter ports. A brouter port is a single-port VLAN that can route IP packets as well as bridge all non-routable traffic. An advantage of this feature is that it eliminates interruptions caused by Spanning Tree Protocol recalculations in routed traffic.

Many to Many Port Mirroring

Many to Many Port Mirroring enables you to use multiple instances of port mirroring simultaneously which allows you to monitor more than one traffic pattern. The ability to monitor multiple traffic patterns is important in networks which support a variety of complex user scenarios, as an example, one port mirror could be set up to allow duplication of VoIP traffic for call recording process, while another instance could be used for intrusion detection and this still allows additional instances for other activities or network troubleshooting.

MLT/DMLT/LAG Dynamic VLAN Changes

Enhancements have been made to the operation of Link Aggregation Groups (LAG) so as to provide consistent operation of Multi-Link Trunk (MLT), Distributed Multi-Link Trunk (DMLT), and LAGs. Now you can make dynamic VLAN changes (that is addition or removal) on any trunks without disabling the trunk first. This is an important improvement in that it allows you to make VLAN changes on any trunks while keeping them in service.

Network Time Protocol (NTP)

The switch now can support either Simple Network Time Protocol (SNTP) or Network Time Protocol (NTP) for time synchronization. NTP is often more widely used to synchronize system clocks to universal standard time as compared to SNTP, as the NTP protocol provides a more reliable and secure means to achieve time synchronization. NTP supports the option to authenticate NTP connections to the server, thereby ensuring a secure means of information exchange from known or trusted servers. You can configure NTP with up to 10 IPv4 servers.

Ping Source Address

For more flexible testing and network setup diagnostics, Ping has been enhanced so that you can specify the IPv4 source address of the outgoing ICMP request. The source address must be one of the active Layer 3 interfaces and you cannot specify the VRRP virtual address as the source address for Ping.

Secure File Transfer Protocol (SFTP)

For secure (SSH) software images, Secure File Transfer supports the downloading of agent and diagnostic image files as well as the transfer of configuration files (binary or ASCII) to and from a SFTP server.

SFP+ and Additional SFP Support

Release 5.6 introduces four Avaya ERS 4800 Series models that support Small Form Factor Pluggable Plus (SFP+) devices. These SFP+ ports support either 1 Gbps or 10 Gbps connectivity based on the installed device.

The following SFP+ devices are supported on the ERS 4800 products:

SFP+ Order Code	Description
AA1403011–E6	1–Port 10 Gigabit-LR SFP+ (LC) Single mode up to 10 km
AA1403013–E6	1–Port 10 Gigabit-ER SFP+ (LC) Single mode up to 40 km
AA1403015–E6	1–Port 10 Gigabit-SR SFP+ (LC) Multi-mode fibre up to 300 m
AA1403017–E6	1–Port 10 Gigabit-LRM SFP+ (LC) Multi-mode fibre up to 220 m
AA1403018–E6	SFP+ direct attach cable 10 m
AA1403019–E6	SFP+ direct attach cable 3 m
AA1403020–E6	SFP+ direct attach cable 5 m

Additionally this release also adds support for four 100 Mbps SFP devices which can be supported in all ERS 4000 models which support lower speed SFPs.

The followig additional SFP devices are supported with the 5.6 Release:

Order Code	Description
AA1419081-E6	100Base-LX SFP, 1310nm, 10km, LC connector
AA1419082-E6	100Base-BX10-U SFP Bidirectional upstream 1310nm TX 10km SFP. Must be deployed with AA1419083-E6 or similar 100Base-BX

Order Code	Description
AA1419083-E6	100Base-BX10-D SFP Bidirectional upstream 1530nm TX 10km. Must be deployed with AA1419082-E6 or similar 100Base-BX
AA1419084-E6	100Base-ZX, 1550nm 70-80km SFP

Show Flash Function

You can use the show flash function in either ACLI or EDM to display FLASH memory capacity and current usage information.

SSH Client

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

SSH RSA Authentication

SSH RSA Authentication provides increased security for Secure Shell (SSH) login and Secure File Transfer Protocol (SFTP) sessions. With this feature, the switch supports RSA public-private key encryption that uses a digital certificate. SSH RSA Authentication is supported when you select the RSA options and is present only on switches running the Secure (SSH) image.

Stack Health Monitoring and Recovery

Stack Health Monitoring and Recovery automatically provides a more robust switch discovery mechanism for stack operation. Additional monitoring and logging information produced by switches in the stack ensure that more information is available to troubleshoot any stack related issues should they arise.

Static FDB MAC Entry

You can use Static FDB MAC Entry to configure a MAC address entry permanently in the Layer 2 Forwarding Database (FDB). A static address does not age out and is saved in the configuration file. You use Static FDB MAC Entry in conjunction with Disable MAC Learning.

Terminal Mode Permanent Setting

With Terminal Mode Permanent Setting, the system saves terminal settings across login sessions. Retaining the terminal settings makes it easier to use scripts to configure or poll the switch.

Trace Functions

The trace command provides a debug feature that facilitates understanding of the execution flow of specifc application modules running on the switch. Trace can be useful for troubleshooting if an application module is not working properly and can be enabled in ACLI either via the console or telnet/SSH connection. The output of the trace command is displayed on the console port.

VLAN Scaling

After upgrading to Release 5.6, the switch/stack supports up to 1,024 concurrent VLANs (from 256 in previous releases) with VIDs in a range from 1 to 4094. With the introduction of VLAN Scaling, ACLI has been enhanced to allow add/delete/membership operations for a group of VLANs allowing faster configuration of a high number of VLANs. If you perform multiple VLAN operations using these new commands, you need to set the VLAN configuration control to flexible, unless the port is ”'tagged” (tagging is tagAll or untagPvidOnly).

Voice VLAN Integration

Voice VLAN Integration provides centralized creation and management of up to 6 Voice VLANs using VLAN-specific commands. With Voice VLAN Integration, each application (e.g. ADAC or EAP) will use these Voice VLANs. For ADAC, this means you must now configure a VLAN as Voice type and be present on the switch before you can configure the ADAC to use that VLAN. As the ADAC VLAN is no longer dynamic, this brings additional benefits in that VLAN membership and configuration can be customized and retained across reboots and that if required, Layer 3 can also be enabled on the ADAC VLAN.

Other changes

See the following sections for information about changes that do not apply to new features:

New Avaya Ethernet Routing Switch 4000 Series models

Release 5.6 introduces the following six new hardware models to the Avaya Ethernet Routing Switch 4000 Series:

- Avaya Ethernet Routing Switch 4550T-PWR+
- Avaya Ethernet Routing Switch 4526T-PWR+
- Avaya Ethernet Routing Switch 4850GTS
- Avaya Ethernet Routing Switch 4850GTS-PWR+
- Avaya Ethernet Routing Switch 4826GTS
- Avaya Ethernet Routing Switch 4826GTS-PWR+

All six new hardware models feature a faster CPU and an increase in FLASH storage size which can allow for large images, backup images, and configurations. These new models also support the new industry standard RJ-45 (8–pin female DTE) serial console port connector.

Release 5.6 also introduces two removable power supplies for the Avaya Ethernet Routing Switch 4000 Series:

- the four PoE+/PWR+ models are shipped with a 1000W AC Power over Ethernet plus power supply unit and a second power supply can be added for redundancy or additional DTE power. The PoE+ models include a 1000W power supply that enables full support for 48 ports when all ports are operating at class 3 802.3af PoE.
- the two 4800 non-PoE+/PWR+ models are shipped with a 300W AC power supply unit and a second power supply can be added for redundancy.

Avaya Identity Engines Ignition Server

Avaya Identity Engines Ignition Server (Ignition Server) is an 802.1X-capable RADIUS authentication server and TACACS+ server that grants or denies users access to your network based on your policies. When you use Ignition Server you can create a single set of policies that control access for all user connection methods: over a wired Ethernet jack, wireless, or VPN.

Ignition Server also authenticates devices and you can configure an 802.1X authentication bypass for older devices on your network that cannot perform an 802.1X authentication.

Diagnostic Auto Unit Replacement (DAUR)

The DAUR feature is disabled in Release 5.6. You can download a diagnostic image through the *download* ACLI command.

Chapter 3: ERS 4000 feature configuration

This chapter contains information about the following Release 5.6 features:

- HTTP/HTTPS port configuration
- IGMP snooping on a VLAN configuration

HTTP/HTTPS port configuration

The Web server can operate in either HTTPS (secure) mode or HTTP (non-secure) mode, with HTTPS as the default mode. You can select the Web server mode with the ACLI and SNMP management interfaces. The SSL Management Library interacts with the Web server in selecting these modes.

In secure mode, you can use the **SecureOnly** option to configure the Web server to respond to HTTPS only, or both HTTPS and HTTP client browser requests. If you configure the Web server to respond to HTTPS client browser requests only, all existing non-secure connections with the browser are terminated.

By default, the Web server listens on TCP port 443 for HTTPS client browser requests, and listens on TCP port 80 for HTTP client browser requests. You can designate alternate TCP ports, ranging in value from 1024 to 65535, for HTTPS and HTTP client browser requests.

Note:

The TCP port for HTTPS client browser requests and the TCP port for HTTP client browser requests cannot be the same value.

In non-secure mode, the Web server responds to HTTP client browser requests only. All existing secure connections with the browser are terminated.

Related topics:

Setting the switch HTTP port using ACLI on page 18
Restoring the switch HTTP port to default using ACLI on page 18
Displaying the switch HTTP port value using ACLI on page 19
Restoring the switch HTTPS port to default using ACLI on page 19
Restoring the switch HTTPS port to default using ACLI on page 20
Displaying the switch HTTP port value using ACLI on page 20
Setting the switch HTTP/HTTPS port using EDM on page 21

Setting the switch HTTP port using ACLI

Use this procedure to set the value for the HTTP port that the switch uses for client Web browser requests.

Before you begin

If the switch is running a secure image, disable SSL.

About this task

Procedure

1. Enter Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:

```
http-port {1024-65535}
```

Related topics:

Variable definitions on page 18

Variable definitions

The following table describes the parameters for the **`http-port`** command.

Variable	Value
{1024–65535}	Specifies a value for the switch HTTP port, ranging from 1024 to 65535. DEFAULT: 80

Restoring the switch HTTP port to default using ACLI

Use this procedure to restore the value for the HTTP port that the switch uses for client Web browser requests to the default value of 80.

About this task

Procedure

1. Enter Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:

```
default http-port
```

Displaying the switch HTTP port value using ACLI

Use this procedure to display the value for the HTTP port that the switch uses for client Web browser requests.

About this task

Procedure

1. Enter Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   show http-port
   ```

Restoring the switch HTTPS port to default using ACLI

Use this procedure to set the value for the HTTPS port that the switch uses for secure client Web browser requests.

Before you begin

If the switch is running a secure image, disable SSL.

Procedure

1. Enter Global Configuration mode.
2. At the command prompt, enter the following command:
   ```
   https-port {1024-65535}
   ```

Related topics:

Variable definitions on page 20

Variable definitions

The following table describes the parameters for the **`https-port`** command.

Variable	Value
{1024–65535}	Specifies a value for the switch HTTPS port, ranging from 1024 to 65535. DEFAULT: 443

Restoring the switch HTTPS port to default using ACLI

Use this procedure to restore the value for the HTTPS port that the switch uses for secure client Web browser requests to the default value of 443.

Procedure

1. Enter Global Configuration mode.
2. At the command prompt, enter the following command:
   ```
   default https-port
   ```

Displaying the switch HTTP port value using ACLI

Use this procedure to display the value for the HTTPS port that the switch uses for secure client Web browser requests.

About this task

Procedure

1. Enter Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   show https-port
   ```

Setting the switch HTTP/HTTPS port using EDM

Use the following procedure to configure HTTP/HTTPS port parameters for the switch:

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **General**.
3. On the **Http/Https** tab, configure the HTTP/HTTPS parameters as required.
4. On the toolbar, click **Apply**.

Variable definitions

The following table describes the fields of Http/Https tab.

Variable	Value
HttpPort	Specifies a value for the switch HTTP port, ranging from 1024 to 65535. The default value is 80.
HttpsPort	Specifies a value for the switch HTTPS port, ranging from 1024 to 65535. The default value is 443.
SecureOnly	Configures the Web server to respond to HTTPS only, or both HTTPS and HTTP client browser requests. **Note:** If you configure the Web server to respond to HTTPS client browser requests only, all existing non-secure connections with the browser are terminated.

IGMP snooping on a VLAN Configuration

If at least one host on a VLAN specifies that it is a member of a group, by default, the Avaya Ethernet Routing Switch 4000 Series forwards to that VLAN all datagrams bearing the multicast address of that group. All ports on the VLAN receive the traffic for that group.

The following figure shows an example of this scenario. Here, the IGMP source provides an IP Multicast stream to a designated router. Because the local network contains receivers, the designated router forwards the IP Multicast stream to the network. Switches without IGMP snoop enabled flood the IP Multicast traffic to all segments on the local subnet. The receivers requesting the traffic receive the desired stream, but so do all other hosts on the network. Although the nonparticipating end stations can filter the IP Multicast traffic, the IP Multicast traffic still exists on the subnet and consumes bandwidth.

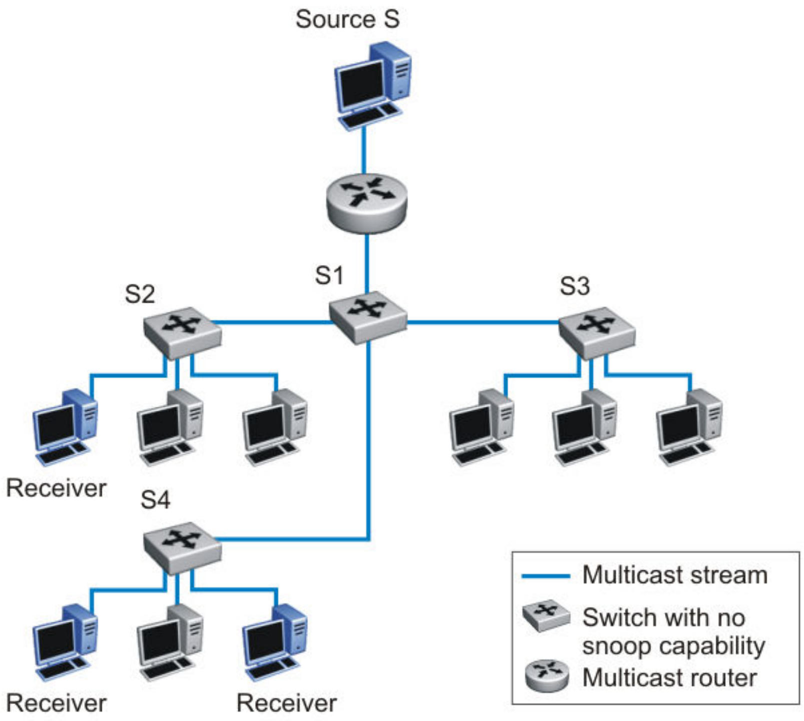

Figure 1: IP multicast propagation on a LAN without IGMP snooping

To prune ports that are not group members from receiving the group data, the Avaya Ethernet Routing Switch 4000 Series supports IGMP snoop for IGMPv1 and IGMPv2. With IGMP snoop enabled on a VLAN, the switch forwards the multicast group data to only those ports that are members of the group. When using IGMP snoop, VLANs can provide the same benefit as IP Multicast routers, but in the local area.

The Avaya Ethernet Routing Switch 4000 identifies multicast group members by listening to IGMP packets (IGMP reports, leaves, and queries) from each port. The switch suppresses the reports by not forwarding them out to other VLAN ports, forcing the members to continuously send their own reports. The switch uses the information gathered from the reports to build a list of group members. After the group members are identified, the switch blocks the IP Multicast stream from exiting any port that does not connect to a group member, thus conserving bandwidth.

As shown in the following figure, after the switches learn which ports are requesting access to the IP Multicast stream, all other ports not responding to the queries are blocked from receiving the IP Multicast data.

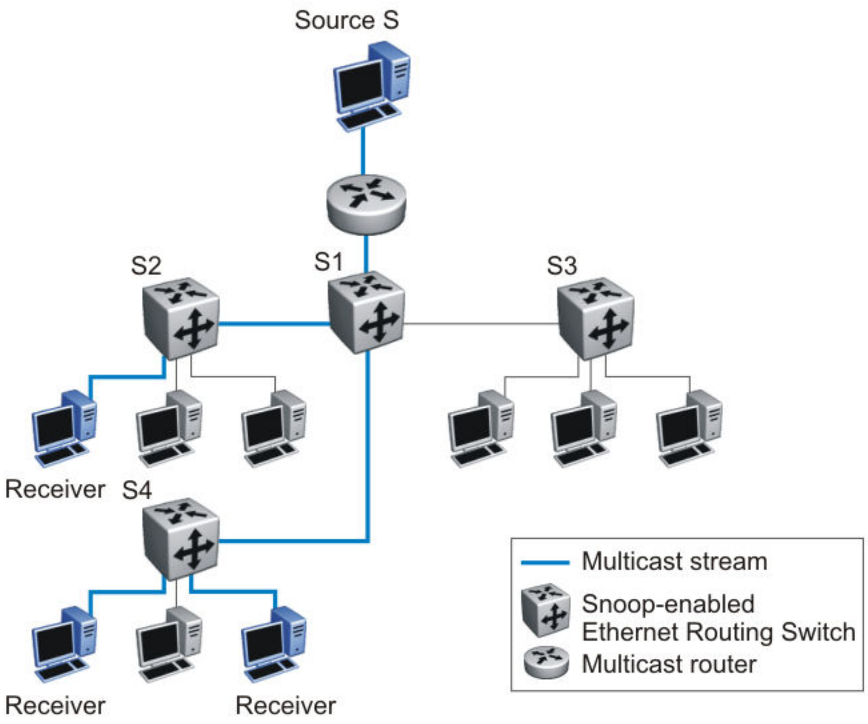

Figure 2: Ethernet Routing Switch running IGMP snooping

The switch continues to forward the IGMP membership reports from the hosts to the multicast routers, and also forwards queries from multicast routers to all port members of the VLAN.

Related topics:

Configuring IGMP snooping on a VLAN on page 23
Configuring VLAN Snoop on page 24

Configuring IGMP snooping on a VLAN

Enable IGMP snooping on a VLAN to forward the multicast data to only those ports that are members of the group.

IGMP snooping is disabled by default.

Related topics:

Procedure steps on page 24
Variable definitions on page 24

Procedure steps

1. Log on to VLAN Interface Configuration command mode in ACLI.
2. Enable IGMP snooping:

```
[default] [no] ip igmp snooping
```

OR

1. Log on to Global Configuration command mode in ACLI:
2. Enable IGMP snooping:

```
[default] vlan igmp <vid> [snooping {enable | disable}]
```

Variable definitions

The following table describes the command variables.

Variable	Value
default	Disables IGMP snooping on the selected VLAN.
no	Disables IGMP snooping on the selected VLAN.
enable	Enables IGMP snooping on the selected VLAN.
disable	Disables IGMP snooping on the selected VLAN.

Configuring VLAN Snoop

Use this procedure to enable or disable IGMP snooping on a switch.

For information on the IGMP snooping feature, refer to *Avaya Ethernet Routing Switch 4000 Series Configuration — IP Routing Protocols*, NN47205-506.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. From the VLAN tree, click **VLANs**.
3. Select the **Snoop** tab.

Variable definitions

The following table outlines the parameters of the **Snoop** tab.

Table 1: VLAN Snoop tab parameters

Variable	Value
Id	Specifies the ID of the VLAN.
ReportProxyEnable	A flag to note whether IGMP Report Proxy is enabled on this VLAN.
Enable	A flag to note whether IGMP Snooping is enabled on this VLAN.
Robustness	Allows tuning for the expected packet loss on a subnet. If a subnet is expected to be *lossy*, the Robustness variable may be increased. IGMP is robust to (Robustness - 1) packet losses.
QueryInterval	Specifies the interval (in seconds) between IGMP Host-Query packets transmitted on this interface.
MRouterPorts	Specifies the set of ports in this VLAN that provide connectivity to an IP Multicast router.
Ver1MRouterPorts	Specifies the version 1 ports in this VLAN that provide connectivity to an IP Multicast router.
Ver2RouterPorts	Specifies the version 2 ports in this VLAN that provide connectivity to an IP Multicast router.
ActiveMRouterPorts	Specifies the active ports.
ActiveQuerier	Specifies the IP address of multicast querier router
QuerierPort	Specifies the port on which the multicast querier router was heard.
MRouterExpiration	Specifies the multicast querier router aging time out

Chapter 4: Important notices

The following sections provide important notices.

Supported software and hardware capabilities

The following table lists supported software and hardware scaling capabilities in Avaya Ethernet Routing Switch 4000 Series Software Release 5.6. The information in this table supersedes information contained in any other document in the suite.

Table 2: Supported software and hardware scaling capabilities

Feature	Maximum number supported
Egress queues	Configurable 1–8
MAC addresses	8,192
Stacking bandwidth (full stack of 8 units)	Up to 384 Gbps
QoS precedence	8 per ASIC
QoS rules per ASIC	128 rules per precedence
Maximum number of units in a stack	8
Maximum number of Port Mirroring Instances	4
Layer 2	
Concurrent VLANs	1,024
Supported VLAN IDs	1 - 4094 (0 and 4095 reserved; 4001 reserved by STP; 4002-4008 reserved by multiple STP groups)
Protocol VLAN types	7
Multi-Link Trunking (MLT), Distributed Multi-Link Trunking (DMLT), and Link Aggregation (LAG) groups	32
Maximum MAC Learning rate on an MLT trunk	500 new MAC addresses per second
Links or ports for MLT, DMLT or LAG	8
Static MAC Addresses	1,024

Feature	Maximum number supported
Spanning Tree Group instances (802.1s)	8
Avaya Spanning Tree Groups	8
DHCP Snooping table entries	1,024
Layer 3	
IP Interfaces (VLANs or Brouter ports)	256
ARP Entries total (local, static & dynamic)	1,792
ARP Entries — local (IP interfaces per switch/stack)	256
ARP Entries — static	256
ARP Entries — dynamic	1,280
IPv4 Routes total (local, static & dynamic)	512
IPv4 Static Routes	32 (configurable 0-256)
IPv4 Local Routes	64 (configurable 2-256)
IPv4 Dynamic Routes (RIP & OSPF)	416 (configurable up to 510)
Dynamic Routing Interfaces (RIP & OSPF)	64
OSPF Areas	4 (3 areas plus area 0)
OSPF Adjacencies (devices per OSPF Area)	16
OSPF Link State Advertisements (LSA)	10,000
OSPF Virtual Links	4
ECMP (Max concurrent equal cost paths)	4
ECMP (Max next hop entries)	128
VRRP Instances	256
Management Routes	4
UDP Forwarding Entries	128
DHCP Relay Entries	256
DHCP Relay Forward Paths	512
Miscellaneous	
IGMP v1/v2 multicast groups	512
IGMP v3 multicast groups	512
IGMP Enabled VLANs	256
802.1x (EAP) clients per port, running in MHMA	32

Feature	Maximum number supported
802.1x (NEAP) clients per switch/stack	384
802.1x (EAP & NEAP) clients per switch/stack	768
Maximum RADIUS Servers	2
Maximum 802.1X EAP Servers	2
Maximum 802.1X NEAP Servers	2
Maximum RADIUS/EAP/NEAP Servers	6
IPFIX number of sampled flows	100,000
LLDP Neighbors per port	16
LLDP Neighbors	800
RMON alarms	800
RMON events	800
RMON Ethernet statistics	110
RMON Ethernet history	249

Filter, meter and counter resources

The following table details filter, meter and counter resources used on the Avaya Ethernet Routing Switch 4000 when various applications are enabled.

Note:

Filters will use the highest available precedence.

Table 3: Filter, meter and counter resources per port

Feature	Observation	QoS			NonQos	
		Filters	Meters	Counter	Filters	Meters
EAPOL		0	0	0	2	0
ADAC		0	0	0	1	0
DHCP Relay	L2 mode	0	0	0	0	0
DHCP Relay	L3 mode	0	0	0	0	0
DHCP Snooping		0	0	0	2	1

Feature	Observation	QoS			NonQos	
NSNA	**Red**					
	Precedence 5	3	1	1	0	0
	Precedence 4	1	1	1	0	0
	Precedence 3	2	1	1	0	0
	Precedence 2	1	1	1	0	0
	Precedence 1	1	1	1	0	0
NSNA	**Yellow**					
	Precedence 6	3	0	1	0	0
	Precedence 5	1	0	1	0	0
	Precedence 4	1	0	1	0	0
	Precedence 3	2	0	1	0	0
	Precedence 2	1	0	1	0	0
	Precedence 1	1	0	1	0	0
NSNA	**Green**					
	Precedence 1	1	0	1	0	0
MAC Security		0	0	0	0	0
IP Source Guard		0	0	1	11	0
Port Mirroring	Mode XrxYtx	1	0	0	0	0
Port Mirroring	XrxYtx or YrxXtx	0	0	0	2	0
Port Mirroring	AsrcBdst, Asrc, Adst	1	0	0	0	0
Port Mirroring	AsrcBdst or BscrAdst, Asrc or Adst	2	0	0	0	0
QoS	Trusted	0	0	0	0	0
QoS	**Untrusted**					
	Precedence 2	1	0	1	0	0
	Precedence 1	1	0	1	0	0
QoS	Unrestricted	0	0	0	0	0
UDP Forwarding		0	0	0	1	1
OSPF		0	0	0	3	0
RIP		0	0	0	1	0

Feature	Observation	QoS			NonQos	
IPFIX		0	0	0	1	1
SLPP Guard		0	0	0	1	1

File names for this release

The following table describes the Avaya Ethernet Routing Switch 4000 Series, Software Release 5.6 software files. File sizes are approximate.

Table 4: Software Release 5.6 components

Module or File Type	Description	File Name	File Size (bytes)
Standard Runtime Software Image	Standard image for the Avaya Ethernet Routing Switch 4000 Series	4000_560008.img	8,474,884
Secure Runtime Software Image	Secure image for the Avaya Ethernet Routing Switch 4000 Series	4000_560009s.img	8,874,252
Diagnostic Software Image	4500 diagnostic image (except 4500–PWR+ models)	4500_53003diag.bin	1,589,514
	4000 diagnostic image (4500–PWR+ & 4800 models)	4000_56015diag.bin	1,931,129
	4000 combination diagnostic image (all 17 models)	4000_56015combodiag.bin	3,520,643
PoE+ Firmware	4000 PoE+ firmware	4000_5600_PoEplus_401B3.bin	16,384
Enterprise Device Manager Help Files	Help files required for Avaya Ethernet	4000_5600_EDMhelp.zip	3,699,150

Module or File Type	Description	File Name	File Size (bytes)
	Routing Switch 4000		
Enterprise Device Manager Plug-in	Avaya Ethernet Routing Switch 4000 Enterprise Device Manager plug-in for Configuration and Orchestration Manager	4000_5600_EDMplugin.zip	4,684,872
Software Release 5.6 Management Information Base (MIB) Definition Files	MIB definition files	4000_5600_MIBs.zip	2,026,887
Demonstration License	Demonstration License	4000_5600_Demo.lic	

Note:

PoE+ firmware for the ERS 4000 models is not required to be downloaded to the PoE+ switch model unless you have a unit which shipped with pre-release software (i.e. shipped before 14 December 2011).

Supported traps and notifications

For information about SNMP traps generated by the Avaya Ethernet Routing Switch 4000 Series, see Avaya *Ethernet Routing Switch 4000 Series Troubleshooting,* (NN47205-700).

Supported Web browsers for Enterprise Device Manager

The following is a list of Internet Web browsers supported by EDM:

- Microsoft Internet Explorer versions 7.0 and 8.0
- Mozilla Firefox version 3.x

For more information about EDM, see *Avaya Ethernet Routing Switch 4000 Series Fundamentals,* (NN47205-101).

Upgrading Software

To upgrade to the new software release 5.6, Avaya recommends that you first verify or upgrade the diagnostics image. For ERS 4500 models (excluding the 4526T-PWR+ and 4550T-PWR+), you are recommended to use version 5.3.0.3 of the diagnostics. For all 4800 as well as the 4526T-PWR+ and 4550T-PWR+ models, use the 5.6.0.15 diagnostics. Once the diagnostics image is verified or updated, you can then upgrade the agent version to release 5.6.

You can download the latest software release from www.avaya.com/support.

The following table describes possible image locations:

Table 5: Possible scenarios

Image	Location
Local Agent Image	Agent image in the flash memory of the unit.
Local Diagnostic Image	Diagnostic image in the flash memory of the unit
5.1.0.7 Diagnostic Image	Diagnostic image released in 5.1
5.2.0.3 Diagnostic Image	Diagnostic image released in 5.2
5.3.0.3 Diagnostic Image	Diagnostic image released in 5.3
5.3.0.3 Diagnostic Image	Diagnostic image released in 5.4
5.3.0.3 Diagnostic Image	Diagnostic image released in 5.5
5.3.0.3 Diagnostic Image for the following units: 4524GT, 4524GT-PWR, 4526FX, 4526GTX, 4526GTX –PWR, 4526T, 4526T-PWR, 4548GT, 4548GT-PWR, 4550T, 4550T-PWR.	Diagnostic image released in 5.6
5.6.0.15 Diagnostic Image for the following units: 4550T-PWR+, 4526T-PWR+, 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+.	Diagnostic image released in 5.6
Combo 5.6.0.15 Diagnostic Image that is a combination between 5.3.0.3 and 5.6.0.15 and can be downloaded on all units.	Diagnostic image released in 5.6

You can upgrade the Agent Image in your switches from an earlier release image.

Important:

You can upgrade any previous release software to the 5.6.0 Agent image. For the six new models introduced in Release 5.6, you must use the 5.6.0 Agent image as the minimum supported software revision either standalone or if the unit is stacked with any other ERS 4000 models.

Important:

A switch that has an agent runtime image prior to release 5.2.0 should not be added directly to a stack running 5.2.0 or later software unless it is running diagnostic image 5.3.0.3 or later. To add a switch with an agent code prior to 5.2.0 to a stack running later software, you should at a minimum upgrade the diagnostic code, on that unit, to at least 5.3.0.3 version and preferably upgrade the agent software before adding the switch to the stack.

Switches with agent runtime software older than 5.2.0 cannot perform an automatic diagnostic upgrade (DAUR) to the version which is operational in the stack. If a switch with software release prior to 5.2 is added into a stack, the unit is not allowed to join the stack and the base unit on that switch will flash rapidly to indicate an issue. The switch system log will provide information that the switch could not be upgraded and had mismatching software.

When loading software release 5.6 it is mandatory that the switches are loaded with either 5.3.0.3, 5.6.0.15 or later diagnostic software due to the increased size of the runtime agent code.

Use the following procedure to upgrade the Agent Image from release 5.0, 5.1, 5.2, 5.3, 5.4 or 5.5 to release 5.6:

Upgrading Agent Image from release 5.0, 5.1, 5.2, 5.3, 5.4, or 5.5 to release 5.6.

1. Upgrade the diagnostic image from the earlier release to release 5.3.0.3 diagnostic image.
2. Upgrade the agent image from release 5.0, 5.1, 5.2, , 5.3, 5.4 or 5.5 to release 5.6 agent image.

Warning:

If you upgrade to release 5.6 which supports 1,024 concurrent VLAN IDs and then downgrade to a prior release of software, the switch configuration defaults. **Workaround**: Save the ASCII configuration before either the upgrade to 5.6 or the downgrade and reload the relevant configuration information after performing the downgrade.

Effects of Upgrade Unified Authentication

With the introduction of Release 5.5 and later Unified Authentication is supported on all ERS 4000 products. With Unified Authentication you can now manage only one set of local usernames and passwords for switches, whether the units are operating in stacked or standalone mode.

The unified authentication mechanism approach simplifies the design: using the current ‘cli password’ and ‘username’ commands the same set of read-write/read-only username and passwords and authentication type is applied to a stack as well as each standalone switch.

The switch obsoletes and clears the switch passwords and username; so that when the unit is operating in either standalone or stacked mode it always uses what was previously designated as the stack password and username.

When downgrading the software image from unified password to an older software image with separate switch and stack passwords all the switch settings (except IP address) will be defaulted, including authentication methods.

Special consideration needs to be given to the upgrade from an older software image with separate switch and stack passwords (any software image previous to 5.5 software image) to a 5.5 or 5.6 software image with unified password. When upgrading from a pre-5.5 software image with separate switch and stack set of credentials (password, username and authentication type) to 5.5, 5.6 or later software image, only the stack set of credentials will be preserved and used; the individual switch set of credentials will be lost and will be overwritten by the new unified/stack set of credentials.

The following message appears in system log :

```
CLI pswd: A unified authentication method is now used. The local
switch credentials are no longer supported.
```

For example, when a standalone unit had previously just the switch set of credentials configured (and no stack credentials), after upgrading to 5.5 or later software the previous stack set of credentials will overwrite the switch set of credentials and as a result the standalone switch will have default settings for the set of credentials.

Setting RADIUS or TACACS+ authentication requires that the switch or stack has a management IP address properly configured, otherwise the user will be locked out of the system because the server providing authentication can never be reached.

Neither RADIUS nor TACACS+ servers can be configured without first having a management IP address. When the user tries to set RADIUS or TACACS+ authentication without having a RADIUS/TACACS+ server configured an error message appears in the console:

```
% You must configure Primary RADIUS Server and shared secret first
% You must configure Primary TACACS+ Server and shared secret first
```

With the unified authentication approach, when configuring RADIUS or TACACS+ on a stack, the authentication type is also applied to each switch within the stack. Consideration needs to be given for removal of a switch from the stack if a standalone switch IP address is not configured. If a switch within a stack does not have a standalone Switch IP address configured, then when either RADIUS or TACACS+ authentication is configured for the stack, this authentication method will not be applied to the respective standalone switch authentication and will only be applied to the stack and any switches with standalone IP addresses. The following log message appears in System log when such a configuration is made in stack:

```
CLI pswd: Stack auth. type RADIUS/TACACS+ won't apply on switch
(switch IP address not set). Local user/password used.
```

Known limitations

For a standalone unit with an switch IP address set but no stack IP address set, if RADIUS or TACACS+ authentication is desired, the command **`cli password serial/telnet radius/tacacs`** will only set this for the standalone operation (and the stack mode will be left at type local). After a reboot the stack credentials will overwrite switch credentials. **Workaround**: To avoid this case, Avaya recommends setting a stack IP address (even on standalone operating mode) before setting authentication type.

Effects of Upgrade on SNMP Trap Notifications

Important:

A new notification control mechanism was introduced with Release 5.4.0 . If you upgrade from an earlier release, all notifications are enabled in Release 5.6, regardless of whether you disabled them prior to the upgrade. When you upgrade from Release 5.5 to Release 5.6 the switch remembers the prior enabled or disabled state of notifications.

You can use the following procedures to restore trap functionality.

To restore trap notification functionality, use the following ACLI procedure:

1. Use the following ACLI command to remove traps created in R5.3:

   ```
   no snmp-server host X.Y.Z.T 'community name'
   ```

2. Reconfigure trap notification, using either ACLI or EDM.

To reconfigure traps, use the following 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.

To reconfigure traps, use the following ACLI procedure—v1 host example with password security enabled:

1. To create a community—from the global configuration prompt, enter the following command:

```
snmp-server community notify-view acli
```

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 filter TestFilter
```

To reconfigure traps, use the following ACLI procedure—v1 host example with password security disabled:

1. To create an SNMP community—from the global configuration prompt, enter the following command:

```
snmp-server community CommunityName notify-view acli
```

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
```

To set the Notification Type per receiver, use the following 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
```

To display the notification types associated with the notify filter, use the following ACLI procedure:

From the global configuration prompt, enter the following command:

```
show snmp-server notification-control
```

To enable or disable the Notification Type per device, use the following 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
```

Updating switch software

You can update the version of software running on the switch through either ACLI or Enterprise Device Manager (EDM).

Before you attempt to change the switch software, ensure that the following prerequisites are in place:

- The switch has a valid IP address and a Trivial File Transfer Protocol (TFTP) or Secure File Transfer Protocol (SFTP) server is on the network that is accessible by the switch and that has the desired software version loaded onto the server.

OR

- If you update the switch software using a USB Mass Storage Device, ensure that the Mass Storage Device has the desired software version and is inserted into the front panel USB port.
- If you use ACLI, ensure that ACLI is in Privileged EXEC mode.

See the following sections for details about updating switch software:

- General software upgrade instructions on page 38
- Changing switch software in ACLI on page 38
- Changing switch software in EDM on page 40

General software upgrade instructions

Use the following procedure to upgrade the Avaya Ethernet Routing Switch 4000 Series software:

1. Backup the binary (and optionally the ASCII) configuration file to a TFTP and/or SFTP server or USB storage device.
2. Upgrade the diagnostic code, if a new version is available. The system will reboot after this step, if you do not specify the **no-reset** option.
3. Upgrade the software image. The system will reboot after this step, if you do not specify the **no-reset** option.
4. If the system was not reset/rebooted after the agent code was updated, you will need to choose a time to reset the system so that the software upgrade will take effect.

Changing switch software in ACLI

Perform the following procedure to change the software version that runs on the switch with ACLI:

1. Access ACLI through the Telnet/SSH protocol or through a Console connection.
2. From the command prompt, use the download command with the following parameters to change the software version:

```
download [{tftp | sftp} address {<A.B.C.D> | <ipv6_address>}]
| usb [unit<unit number>] diag <WORD> | image <WORD> | image-
if-newer <WORD> | poe_module_image <WORD>} [username <WORD>
[password] [no-reset]
```

3. Press `Enter`.

The software download 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 or power off the unit during the download process. Depending on network conditions, this process may take up to 8 minutes if performing an agent code update in a large stack configuration.

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

Important:

During the download process, the management functionality of the switch is locked to prevent configuration changes or other downloads. Normal switching operations will continue to function while the download is in progress.

Job aid—download command parameters

The following table describes the parameters for the **`download`** command.

Table 6: ACLI download command parameters

Parameter	Description
The image, image-if-newer, diag, and poe_module_image parameters are mutually exclusive; you can execute only one at a time. The address <ip> and usb parameters or tftp and sftp parameters are mutually exclusive; you can execute only one at a time.	
tftp address <ipv6 address> | <ipv4 address>	The IPv4 or IPv6 address of the TFTP server you use. The address <ipv6_address> | <ipv4_address> parameter is optional and if you omit it, the switch defaults to the TFTP server specified by the **`tftp-server`** command.
sftp address <ipv6 address> | <ipv4 address>	The IPv4 or IPv6 address of the SFTP server you use. The address <ipv6_address> | <ipv4_address> parameter is optional and if you omit it, the switch defaults to the SFTP server specified by the **`sftp-server`** command. When using SFTP, the username parameter can be utilized. **Note**: SFTP transfer is only possible when

Parameter	Description
	the switch/stack is running the secure software image.
usb [unit <unit number>]	Specifies that the software download is performed using a USB Mass Storage Device and the front panel USB port. Use the unit number parameter to specify which switch contains the USB in a stack.
image <*image name*>	The name of the software image to be downloaded from the TFTP/SFTP server or USB Mass Storage Device.
image-if-newer <*image name*>	This parameter is the name of the software image to be downloaded from the TFTP/SFTP server or USB Mass Storage Device if it is newer than the currently running image.
diag <*image name*>	The name of the diagnostic image to be downloaded from the TFTP/SFTP server or USB Mass Storage Device.
poe_module_image <*image name*>	The name of the Power over Ethernet plus firmware to be downloaded from the TFTP/SFTP server or USB Mass Storage Device. This option is available only for 4000 Series switches that support Power Over Ethernet plus.
no-reset	This parameter forces the switch to not reset after the software download is complete.
username <username> [password]	Specifies the username and optionally the password which can be used when connecting to the SFTP server. No password is required if DSA or RSA keys have been appropriately configured.

Changing switch software in EDM

Use the following procedure to change the software version running on the switch that uses EDM.

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

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

Do not interrupt the download or power off the unit during the download process. Depending on network conditions, this process may take up to 8 minutes if performing an agent code update in a large stack configuration

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

Important:

During the download process, the management functionality of the switch is locked to prevent configuration changes or other downloads. Normal switching operations will continue to function while the download is in progress.

Job aid—File System screen fields

The following table describes the File System screen fields.

Table 7: File System screen fields

Field	Description
TftpServerInetAddress	Indicates the IP address of the TFTP or SFTP* server on which the new software images are stored for download.
TftpServerInetAddressType	Indicates the type of TFTP or SFTP* server address type: • IPv4 • IPv6
BinaryConfigFileName	Indicates the binary configuration file currently associated with the switch. Use this field when you work with configuration files; do not use this field when you download a software image.
BinaryConfigUnitNumber	When in standalone mode, and loading a binary configuration file that was created from a stack, this object specifies the unit number of the portion of the configuration file to be extracted and used for the standalone unit configuration. If this value is 0, it is ignored.
ImageFileName	Indicates the name of the image file currently associated with the switch. If needed, change this field to the name of the software image to be downloaded.
FwFileName (Diagnostics)	The name of the diagnostic file currently associated with the switch. If needed, change this

Field	Description
	field to the name of the diagnostic software image to be downloaded.
UsbTargetUnit	Indicates the unit number of the USB port to be used to upload or download a file. A value of 0 indicates download is via TFTP; a value of 9 indicates a standalone switch and a value of 10 indicates SFTP* server.
Action	This group of options represents the actions taken during this file system operation. The options applicable to a software download are • dnldConfig: Download a configuration to the switch. • dnldConfigFromSftp: Download a configuration to switch from the SFTP Server*. • dnldConfigFromUsb: Download a configuration to switch using the front panel USB port. • dnldFw: Download a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. • dnldFwFromSftp: Download a new diagnostic software image to the switch from the SFTP server. This option replaces the image regardless of whether it is newer or older than the current image*. • dnldFwFromSftpNoReset: Download a new diagnostic software image to the switch from the SFTP server. This option replaces the image regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset*. • dnldFwFromUsb: Download a new diagnostic software image to the switch from the front panel USB port. This option replaces the image regardless of whether it is newer or older than the current image. • dnldFwNoReset: Download a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset. • dnldImg: Download a new software image to the switch. This option replaces the software image

Field	Description
	on the switch regardless of whether it is newer or older than the current image. • dnldImgFromSftp: Download a new software image to the switch from the SFTP server. This option replaces the image regardless of whether it is newer or older than the current image*. • dnldImgFromSftpNoReset: Download a new software image to the switch from the SFTP server. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset*. • dnldImgFromUsb: Download a new software image to the switch using the front panel USB port. This option replaces the image regardless of whether it is newer or older than the current image. • dnldImgIfNewer: Download a new software image to the switch only if it is newer than the one currently in use. • dnldImgNoReset: Download a new software image to the switch. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset. • upldConfig: Upload a configuration to the switch from a designated location. • upldConfigToSftp: Upload binary config to SFTP server*. • upldConfigToUsb: Upload binary config to USB port • upldImgToUsb: Upload image to USB port
Status	Display the status of the last action that occurred since the switch last booted. The values that are displayed are • other: No action occurred since the last boot. • inProgress: The selected operation is in progress. • success: The selected operation succeeded. • fail: The selected operation failed.

* Note: SFTP functions are only supported when running the Secure software image.

Setting IP parameters with the ip.cfg file on a USB memory device

You can load the ip.cfg file from the USB memory device as a means of pre-staging the IP address and other parameters for the operation of a switch.

You can specify one or more of the optional parameters in the ip.cfg file.

The following table describes the ip.cfg file parameters:

Table 8: ip.cfg file optional parameters

Parameter	Description
IP <*xx.xx.xx.xx*>	Specifies the IP address for the switch. Example: 192.168.22.1
Mask <*xx.xx.xx.xx*>	Specifies the network mask. Example: 255.255.255.0
Gateway <*xx.xx.xx.xx*>	Specifies the default gateway. Example: 181.30.30.254
SNMPread <*string*>	Specifies the SNMP read community string. Example: public
SNMPwrite <*string*>	Specifies the SNMP write community string. Example: private
VLAN <*number*>	Specifies the management VLAN-ID. Example: VLAN 1
USBdiag <*string*>	Specifies the file name of the diagnostic image to load from the USB device. Example: ers4000/4000_5.3.0.34.bin
USBascii <*string*>	Specifies the file name of the ASCII configuration file to load from the USB device. Example: customer1.cfg
USBagent <*string*>	Specifies the file name of the runtime agent image to load from the USB device. Example: ers4000/4000_560008.img
NEXTIP, NEXTMask, and NEXTGateway	Specifies IP addresses, network mask and gateway to be used once the switch is rebooted.

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

If you boot up an ERS 4000 switch in factory default configuration with a USB Mass Storage device inserted which contains the following example ip.cfg file, the stack IP becomes 181.30.30.113 with the appropriate mask and gateway regardless of what IP address is in the config.txt file, as the IP commands are processed after the ASCII file is processed:

```
USBascii config.txt
IP 181.30.30.113
Mask 255.255.255.0
Gateway 181.30.30.254
```

If the ip.cfg file contains commands (as follows) where the IP information is specified before any ASCII scripts, then the IP Address will be what is specified in the ip.cfg or if the ASCII file contains IP address commands these will take precedence as they are processed last:

```
IP 181.30.30.113
Mask 255.255.255.0
Gateway 181.30.30.254
USBascii ip.txt
```

It should be noted that if the ip.cfg file specifies an image or agent code, the switch loads the software, even if the same version is already installed on the switch. This is the correct operation of the system as ip.cfg ensures that the appropriate software is always upgraded on the units.

The Avaya Ethernet Routing Switch 4000 restarts with factory default settings and attempts to read the ip.cfg file from an installed USB drive within three minutes. The Avaya Ethernet Routing Switch 4000 banner page appears while the switch retrieves the ip.cfg file.

Important:

To use the ip.cfg capability, the switch must be in default configuration and a USB stick with the ip.cfg file in the root directory must be present. The switch will attempt to read the ip.cfg if present within the first 3 minutes of switch operation. If a console is connected to the switch during the boot process and you require ip.cfg to operate, then DO NOT attempt to access the switch for at least three minutes. This is necessary to give the switch sufficient time to detect and process ip.cfg functions.

The system does not display a message to indicate the ip.cfg file download from the USB memory device is in progress.

Use the following procedure to check the status of the download three minutes after the Avaya banner page displays:

Press `CTRL` and `y` keys together.

Two possible responses indicate a pass or fail status.

- Pass: The system provides an ACLI prompt.

- Fail: The system prompts you for an IP address.

You can confirm the successful download with the **`show ip`** command. If the USB ip.cfg file download succeeded, all parameters read from the ip.cfg file show as present in the switch and become part of the runtime configuration.

Save the configuration with the ACLI command, **`copy config nvram`**. After the successful ip.cfg file download from the USB memory device, you can manage the switch through Telnet and SNMP.

If you load any diagnostic or agent images with ip.cfg, you must have the diagnostic or agent images on the same USB memory device. To ensure that diagnostic and agent image downloaded successfully, check in the system log or audit log.

Hardware and software compatibility

This section provides hardware and software compatibility information.

XFP, SFP and SFP+ Transceiver Compatibility

The following table lists the XFP, SFP and SFP+ transceiver compatibility.

Table 9: XFP and SFP transceiver compatibility

Supported XFPs, SFPs and SFP+s	Description	Minimum software version	Part Number
Small Form Factor Pluggable (SFP) transceivers			
1000BASE-SX SFP	850 nm LC connector	5.0.0	AA1419013-E5
1000BASE-SX SFP	850 nm MT-RJ connector	5.0.0	AA1419014-E5
1000BASE-LX SFP	1310 nm LC connector	5.0.0	AA1419015-E5
1000BASE-CWDM SFP	1470 nm LC connector, up to 40 km	5.0.0	AA1419025-E5
1000BASE-CWDM SFP	1490 nm LC connector, up to 40 km	5.0.0	AA1419026-E5
1000BASE-CWDM SFP	1510 nm LC connector, up to 40 km	5.0.0	AA1419027-E5
1000BASE-CWDM SFP	1530 nm LC connector, up to 40km	5.0.0	AA1419028-E5

Supported XFPs, SFPs and SFP+s	Description	Minimum software version	Part Number
1000BASE-CWDM SFP	1550 nm LC connector, up to 40 km	5.0.0	AA1419029-E5
1000BASE-CWDM SFP	1570 nm LC connector, up to 40 km	5.0.0	AA1419030-E5
1000BASE-CWDM SFP	1590 nm LC connector, up to 40 km	5.0.0	AA1419031-E5
1000BASE-CWDM SFP	1610 nm LC connector, up to 40 km	5.0.0	AA1419032-E5
1000BASE-CWDM SFP	1470 nm LC connector, up to 70 km	5.0.0	AA1419033-E5
1000BASE-CWDM SFP	1490 nm LC connector, up to 70 km	5.0.0	AA1419034-E5
1000BASE-CWDM SFP	1510 nm LC connector, up to 70 km	5.0.0	AA1419035-E5
1000BASE-CWDM SFP	1530 nm LC connector, up to 70 km	5.0.0	AA1419036-E5
1000BASE-CWDM SFP	1550 nm LC connector, up to 70 km	5.0.0	AA1419037-E5
1000BASE-CWDM SFP	1570 nm LC connector, up to 70 km	5.0.0	AA1419038-E5
1000BASE-CWDM SFP	1590 nm LC connector, up to 70 km	5.0.0	AA1419039-E5
1000BASE-CWDM SFP	1610 nm LC connector, up to 70 km	5.0.0	AA1419040-E5
1000BSE-T SFP	Category 5 copper unshielded twisted pair (UTP), RJ-45 connector	5.0.0	AA1419043-E5
1000BASE-SX DDI SFP	850 nm DDI LC connector	5.2.0	AA1419048-E6
1000BASE-LX DDI SFP	1310 nm DDI LC connector	5.2.0	AA1419049-E6
1000BaseXD DDI SFP	1310nm LC connector	5.4.0	AA1419050-E6
1000BaseXD DDI SFP	1550nm LC connector	5.4.0	AA1419051-E6

Supported XFPs, SFPs and SFP+s	Description	Minimum software version	Part Number
1000BaseZX DDI SFP	1550nm LC connector	5.4.0	AA1419052-E6
1000BaseCWDM SFP	1470nm LC connector, up to 40km	5.4.0	AA1419053-E6
1000BaseCWDM DDI SFP	1490nm LC connector, up to 40km	5.4.0	AA1419054-E6
1000BaseCWDM DDI SFP	1510nm LC connector, up to 40km	5.4.0	AA1419055-E6
1000BaseCWDM DDI SFP	1530nm LC connector, up to 40km	5.4.0	AA1419056-E6
1000BaseCWDM DDI SFP	1570nm LC connector, up to 40km	5.4.0	AA1419058-E6
1000BaseCWDM DDI SFP	1590nm LC connector, up to 40km	5.4.0	AA1419059-E6
1000BaseCWDM DDI SFP	1610nm LC connector, up to 40km	5.4.0	AA1419060-E6
1000BaseCWDM DDI SFP	1470nm LC connector, up to 70km	5.4.0	AA1419061-E6
1000BaseCWDM DDI SFP	1490nm LC connector, up to 70km	5.4.0	AA1419062-E6
1000BaseCWDM DDI SFP	1510nm LC connector, up to 70km	5.4.0	AA1419063-E6
1000BaseCWDM DDI SFP	1530nm LC connector, up to 70km	5.4.0	AA1419064-E6
1000BaseCWDM DDI SFP	1550nm LC connector, up to 70km	5.4.0	AA1419065-E6
1000BaseCWDM DDI SFP	1570nm LC connector, up to 70km	5.4.0	AA1419066-E6
1000BaseCWDM DDI SFP	1590nm LC connector, up to 70km	5.4.0	AA1419067-E6
1000BaseCWDM DDI SFP	1610nm LC connector, up to 70km	5.4.0	AA1419068-E6
1000BASE-BX bidirectional SFP	1310 nm, single fiber LC (Must be paired with AA1419070-E5)	5.2.0	AA1419069-E5

Supported XFPs, SFPs and SFP+s	Description	Minimum software version	Part Number
1000BASE-BX bidirectional SFP	1490 nm, single fiber LC (Must be paired with AA1419069-E5)	5.2.0	AA1419070-E5
1000Base DDI SFP	1550nm LC connector, 120 km	5.4.0	AA1419071-E6
100BASE-FX SFP	1310 nm LC connector	5.0.0	AA1419074-E6
100BASE-LX SFP	100Base-LX SFP, 1310nm, 10km, LC connector	5.6.0	AA1419081-E6
100BASE-BX SFP	100Base-BX10-U SFP Bidirectional upstream 1310nm TX 10km SFP (Must be deployed with AA1419083-E6 or similar 100Base-BX).	5.6.0	AA1419082-E6
100BASE-BX SFP	100Base-BX10-D SFP Bidirectional upstream 1530nm TX 10km (Must be deployed with AA1419082-E6 or similar 100Base-BX).	5.6.0	AA1419083-E6
100BASE-ZX SFP	100Base-ZX, 1550nm 70-80km SFP	5.6.0	AA1419084-E6
T1 SFP	1.544 Mbps Fast Ethernet to T1 remote bridge, RJ-48C	5.1.0	AA1419075-E6
1000BASE-BX SFP	1310nm LC connector, up to 40km (Must be paired with AA1419077-E6)	5.3.0	AA1419076-E6
1000BASE-BX SFP	1490nm LC connector, up to 40km (Must be paired with AA1419076-E6)	5.3.0	AA1419077-E6
10 Gigabit Ethernet XFP Transceivers			
10GBASE-LR/LW XFP	1-port 1310 nm SMF, LC connector	5.2.0	AA1403001-E5
10GBASE-SR XFP	1-port 850 nm MMF, LC connector	5.1.0	AA1403005-E5

Supported XFPs, SFPs and SFP+s	Description	Minimum software version	Part Number
10GBASE-ZR/ZW XFP	1550 nm SMF LC connector	5.1.0	AA1403006-E5
10GBASE-LRM XFP	1310 nm, up to 220 m over MMF, DDI	5.2.0	AA1403007-E6
10 Gigabit Ethernet SFP+ Transceivers			
10GBASE-LR SFP+	1–Port 10 Gigabit-LR SFP+ (LC) Single mode up to 10 km	5.6.0	AA1403011–E6
10GBASE-ER SFP+	1–Port 10 Gigabit-ER SFP+ (LC) Single mode up to 40 km	5.6.0	AA1403013–E6
10GBASE-SR SFP+	1–Port 10 Gigabit-SR SFP+ (LC) Multi-mode fibre up to 300 m	5.6.0	AA1403015–E6
10GBASE-LRM SFP+	1–Port 10 Gigabit-LRM SFP+ (LC) Multi-mode fibre up to 220 m	5.6.0	AA1403017–E6
10GDAC-10M SFP+	SFP+ direct attach cable 10 m	5.6.0	AA1403018–E6
10GDAC-3M SFP+	SFP+ direct attach cable 3 m	5.6.0	AA1403019–E6
10GDAC-5M SFP+	SFP+ direct attach cable 5 m	5.6.0	AA1403020–E6

For more information, see *Avaya Ethernet Routing Switch 4000 Series Installation*, (NN47205-300).

Supported standards, RFCs and MIBs

The following sections list the standards, RFCs and MIBs supported in Release 5.6.

Standards

The following IEEE Standards contain information pertinent to the Avaya Ethernet Routing Switch 4000 Series:

- IEEE 802.1 (Port VLAN, Port & Protocol VLANs, VLAN Name, Protocol Entity)
- IEEE 802.1AB (Link Layer Discovery Protocol)
- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1s (Multiple Spanning Trees)
- IEEE 802.1v (VLAN Classification by Protocol and Port)
- IEEE 802.1w (Rapid Reconfiguration of Spanning Tree)
- IEEE 802.1X (EAPOL)
- IEEE 802.3 (Ethernet)
- IEEE 802.3ab (1000BASE-T)
- IEEE 802.3ab (Gigabit Ethernet over Copper)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3ae (10Gb/s Ethernet)
- IEEE 802.3ae (10GBASE-LR/SR/LM)
- IEEE 802.3af (Power over Ethernet)
- IEEE 802.3at (Power over Ethernet)
- IEEE 802.3u (100BASE-FX)
- IEEE 802.3u (100BASE-TX)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (1000BASE-SX)
- IEEE 802.3z (1000BASE-x)
- IEEE 802.3z (Gigabit Ethernet over Fiber-Optic)
- IEEE P802.3ak (10GBASE-CX4)

RFCs and MIBs

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

- RFC 768 (UDP)
- RFC 791 (IP)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 826 (ARP)
- RFC 854 (Telnet)
- RFC 894 (IP over Ethernet)
- RFC 951 (BootP)
- RFC 1058 (RIP v1)
- RFC 1112 (IGMPv1)
- RFC 1157 (SNMP)
- RFC 1213 (MIB-II)
- RFC 1271 (RMON)
- RFC 1305 (Network Time Protocol Version 3)
- RFC 1350 (TFTP)
- RFC 1493 (Bridge MIB)
- RFC 1583 (OSPF v2)
- RFC 1757 (RMON)
- RFC 1850 (OSPF v2 MIB)
- RFC 1945 (HTTP v1.0)
- RFC 2131 (BootP/DHCP Relay Agent)
- RFC 2236 (IGMPv2)
- RFC 2328 (OSPF v2)
- RFC 2453 (RIP v2)
- RFC 2474 (Diffserv)
- RFC 2475 (Diffserv)
- RFC 2665 (Ethernet MIB)

- RFC 2674 (Q-BRIDGE-MIB)
- RFC 2715 (Interoperability Rules for Multicast Routing Protocols)
- RFC 2737 (Entity MIBv2)
- RFC 2819 (RMON MIB)
- RFC 2863 (Interfaces Group MIB)
- RFC 2865 (RADIUS)
- RFC 2866 (RADIUS Accounting)
- RFC 2933 (Internet Group Management Protocol MIB)
- RFC 3046 (DHCP Relay Agent Information Option)
- RFC 3246 (Expedited Forwarding Behavior)
- RFC 3376 (Internet Group Management Protocol, Version 3)
- 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 3569 (An Overview of Source-Specific Multicast [SSM])
- RFC 3576 (Dynamic Authorization Extensions to Remote Authentication Dial In User Service [RADIUS])
- RFC 3768 (Virtual Router Redundancy Protocol)
- RFC 3917 (IP Flow Information Export [IPFIX])
- RFC 3954 (Netflow Services Export v9)
- RFC 3993 (DHCP Subscriber-ID suboption)
- RFC 4250 (The Secure Shell [SSH] Protocol Assigned Numbers)
- RFC 4251 (The Secure Shell [SSH] Protocol Architecture)
- RFC 4252 (The Secure Shell [SSH] Authentication Protocol)
- RFC 4253 (The Secure Shell [SSH] Transport Layer Protocol) -
- RFC 4254 (The Secure Shell [SSH] Connection Protocol)
- RFC 4541 (Considerations for Internet Group Management Protocol [IGMP] and Multicast Listener Discovery [MLD] Snooping Switches)
- RFC 4604 (Using Internet Group Management Protocol Version 3 [IGMPv3])

- RFC 4673 (RADIUS Dynamic Authorization Server MIB)
- RFC 5905 (Network Time Protocol Version 4)

IPv6 specific RFCs

The following lists supported IPv6 specific RFCs:

- RFC 1886 DNS Extensions to support IPv6
- RFC 1981 Path MTU Discovery for IPv6
- RFC 2460 Internet Protocol v6 (IPv6) Specification
- RFC 2461 Neighbor Discovery for IPv6
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 3162 RADIUS and IPv6
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4291 IPv6 Addressing Architecture

The following table lists partially supported IPv6 specific RFCs:

Table 10: Partially Supported IPv6 specific RFCs

Standard	Description	Compliance
RFC 2462	IPv6 Stateless Address Auto-configuration	Auto-configuration of link local addresses only
RFC 2462	Auto-configuration of link local addresses	Supports creation of link-local addresses in section 5.3, and duplicate address detection in section 5.4.
RFC 4007	Scoped Address Architecture	Supports some behavior such as source address selection when transmitting packets to a specific scope, but there is not a zone concept in the code.
RFC 4022	Management Information Base for TCP	Mostly supported.
RFC 4113	Management Information Base for UDP	Mostly supported.
RFC 4213	Transition Mechanisms for IPv6 Hosts and Routers	Supports dual stack. No support for tunneling yet.

Standard	Description	Compliance
RFC 4291	IPv6 Addressing Architecture	Supports earlier version of RFC (3513).
RFC 4293	Management Information Base for IP	Mostly supported.
RFC 4443	Internet Control Message Protocol (ICMPv6)	Supports earlier version of RFC (2463).

Chapter 5: Resolved issues

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

Resolved Issues for Release 5.6

The following table lists the issues resolved for release 5.6.

Reference number	Description
wi00881470	**802.1AB (LLDP), Avaya TLV**: The information pertaining to Avaya proprietary TLVs of dot1q-framing and poe-conservation-request-level are now correctly displayed after reset of a unit within the stack.
wi00881813, wi00881816	**802.1AB (LLDP)**: If you reboot the Base Unit of a stack and then issue the command **`show lldp vendor-specific avaya dotlq-framing`** on the Temporary Base Unit, the switches in the stack will no longer reset.
wi00881821, wi00881822	**802.1AB (LLDP)**: Information is now correctly displayed for 802.1AB (LLDP) MED TX-TLV after a unit in the stack is powered down.
wi00864797, wi00862420,	**802.1AB (LLDP)**: A memory leak which would occur in certain scenarios where the switch is processing a lot of 802.1AB (LLDP) packets is now addressed.
wi00928236	**802.1AB (LLDP)**: When the stack is operating in Temporary Base Unit mode, you can now correctly change 802.1AB (LLDP) TLV information on units within the stack.
wi00862985	**802.1AB LLDPPDUs**: In simulations where high amounts of LLDPPDUs being generated, the stack continues to operate normally.
wi00931113	**802.1X, EAP, DHCP, Guest VLAN**: Devices which are connected to the Non-Base unit in a stack will now correctly receive a DHCP address when they are assigned into the Guest VLAN.
wi00827431	**802.1X, EAP, DHCP, Guest VLAN**: When the switch is booting, DHCP requests are no longer forwarded until 802.1X authentication is established or the device is placed into the Guest VLAN.
wi00895233	**802.1X, EAP**: During periods of high end device authentication (for example at the commencement of the business day where a customer has a large number of users on a stack of 8 switches) the end devices

Reference number	Description
	are now correctly authenticated against the RADIUS server even if the RADIUS queue should become full awaiting responses from the server.
wi00895688	**802.1X, EAP**: Entries for 802.1X / EAP clients are now correctly aged out of the switch as well as the Layer 2 forwarding database (FDB) when devices are removed from the port or moved to a new port.
wi00882779	**ADAC**: A memory leak which could occur when running ADAC in certain scenarios where IP Phones are repeatedly power cycled through disabling and then re-enabling PoE is now addressed.
wi00930103	**ADAC**: When ADAC is configured to use one port of a MLT group as an uplink and the configuration is updated to add the other MLT links as an ADAC uplink, the Voice VAN is now correctly applied to all MLT ports rather than being removed from both MLT uplinks.
wi00885951	**Autotopology, SONMP** : If the Ethernet Routing Switch 4000 is connected to ERS 8800 with 8895CPU or 8810/8806,8803R chassis, the ERS 4000 will now correctly report these devices in the SONMP autotopology table.
wi00491271, wi00484313	**BX SFPs**: When you connect two BX SFPs (Part Code AA1419069-E6 and AA1419070-E6) between Gigabit ERS 4000 switches, a link issue which occurred if the vendor of the BX SFP is Luminet revision A (as identified by the vendor serial number starting with LUMNT) is now rectified.
wi00840626	**CLI, Password, Username**: When issuing commands cli password switch read-write/read-only the following message will appear: `% CLI password: Switch authentication parameter is obsolete, changes have not been applied.` Changes have been applied, see Unified Authentication for more details about new command syntax.
wi00855310	**EAP, NEAP IP Phone, DHCP Signature**: EAP authentication by DHCP signature now works correctly for legacy Avaya (Nortel) IP Phones and Avaya IP Phones.
wi00483813	**EDM, Energy Saver**: EDM now correctly displays the PoE Savings and PoE Priority in the energy saver ports tab.
wi00875776	**EDM, LLDP**: Neighbor PoE information is now available and correctly displayed in EDM.
wi00855367	**EDM, Syslog**: EDM now supports the ability to configure syslog support under Configuration -> Edit -> Diagnostics -> System Log.
wi00876301	**EDM**: EDM now supports the configuration of http &/or https server mode.
wi00489779	**EDM**: EDM now supports the creation of Static MAC addresses in the Layer 2 FDB / MAC Address Table.

Reference number	Description
wi00843413	**EDM**: In the Interface tab, the 1000Half option is now correctly disabled if autonegotiation is enabled.
wi00862831	**Hotswap, SNMP Trap**: When a unit is replaced in a stack, the SNMP Trap s5CtrHotSwap is now correctly generated.
wi00838002	**IGMP Snooping & Proxy**: When issuing the default VLAN command, all IGMP parameters are now correctly set to their default values.
wi00863415	**IPFIX**: A template packet is now correctly sent to the IPFIX collector when enabling IPFIX globally.
wi00869476, wi00928619	**MAC MAC Security**: MAC addresses are now correctly deleted when the `no mac-security mac-address-table` command is issued.
wi00664779	**Management VLAN**: The ifAdminStatus and ifOperStatus MIB objects now provide the correct operational status of the management VLAN if the Management VLAN is operating in Layer 2 mode only.
wi00875002	**Management VLAN**: Irrespective of the state of IP routing on the switch, as soon as a port in the Management VLAN is active the ifOperStatus and ipAdEntIfIndex will now correctly respond as UP.
wi00483626	**MLT/DMLT**: It is now possible to change the VLAN membership of MLT/DMLT & LAG ports while in-service. If you change the VLAN assignment on administratively disabled MLT/DMLT ports, the system prevents them from being added back into the MLT/DMLT group because the VLAN assignments of the links within the groups are inconsistent.
wi00863190	**NEAP, Interim Updates**: When Interim updates are enabled for non-EAP (NEAP) clients, duplicate interim-update with all values set to null are no longer produced.
wi00907963	**Non-Base Unit Reset, ARP**: When the Non-Base Unit in a stack is reset, the ARP entries for end devices are now correctly refreshed and connectivity reestablished without manual intervention.
wi00862952	**OSPF**: In some configurations with multiple devices running OSPF over multiple OSPF Areas routes now correctly recover after link failure and re-establishment.
wi00872828	**OSPF**: When issuing the `show ip ospf stats` command, the LSDB Table size is now correctly displayed.
wi00872224	**PoE Traps**: The pethPsePortOnOffNotification trap is now correctly not able to be configured on a non-PoE switch if that unit is the base unit.
wi00877870	**PoE, ESD**: In certain situations when the Power over Ethernet (PoE) was reset due to excessive Electrostatic Discharge (ESD) power is now correctly reapplied to end devices.

Reference number	Description
wi00862300	**QoS, ADAC**: When ADAC and Auto QoS are both enabled, the QoS marking of the traffic destined for the ADAC Call Server or Uplink ports is now correctly marked.
wi00850218	**RPSU, Software Exception**: In a simulation environment the resetting of the PSU15 supplying power to a non-base unit will no longer cause a software exception on that unit.
wi00882592	**Secure Software Upgrade, Very Large Configurations**: When performing an upgrade to a stack running the Secure software image with a very large configuration, the configuration will no longer become corrupted during the upgrade process.
wi00866308	**SFP**: A third party Encryption SFP (EG1) from Infoguard now correctly works and performs auto-negotiation with an ERS 4500 switch.
wi00934144, wi00491271	**Shared port, SFP**: New shared port functionality using the **`shared-port auto-select`** command is now supported on the 4526GTX, 4526GTX-PWR, 4548GT, and 4548GT-PWR which allows customers to force the selection of either the copper 10/100/1000 port or the SFP port.
wi00832588	**Shared Ports, EDM**: If a SFP is inserted into a shared port, the port now shows correctly in Enterprise Device Manager (EDM) and the associated MIB entries display as being active.
wi00840871	**Unified Authentication**: An improved error message is displayed when deleting an IP address and Radius or TACACS+ Authentication is enabled.
wi00907462	**VLAN, CPU Utilization**: In some configurations with over 740 VLANs configured, the CPU utilization of the switch now no longer maintains 100% while performing a **`show running-config`** command.

Chapter 6: Known Issues and Limitations

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

Known Issues and Limitations for Release 5.6

The following table lists known issues and limitations for Avaya Ethernet Routing Switch 4000 Series Software Release 5.6 and prior releases.

Reference Number	Description
Known issues for Release 5.6	
wi00897222	**802.1AB (LLDP)**: If displaying the status for LLDP dot1 transmission flags in a stack which have 1024 VLANs configured, this will take considerably longer if you use the console port of a Non-Base Unit in the stack. **Workaround**: Avaya recommends that you perform all configuration and display using the console port on the Base Unit of a stack.
wi00959485	**Autotopology, SONMP**: If the Ethernet Routing Switch 4000 is connected to a Virtual Service Platform 7000 (VSP 7000), the ERS 4000 will display the VSP 7000 in the autotopology table as `unknown`.
wi00909985	**AUR, QoS**: When AUR performs an update of a replacement unit if all ports are set to QoS trusted mode and all QoS precedences are used, it may be possible that the QoS parameters will not be correctly restored to the replacement unit. **Workaround**: Save QoS configurations of the stack offline and if this situation occurs, then reapply the configuration file directly to the affected unit.
wi00887780	**Brouter Ports**: When you create brouter ports, if the maximum number of IP interfaces is reached, the following message will be displayed in ACLI: `%Maximum IP interfaces are already configured`. In this case the system will not create the brouter port, however the port may be removed from the initial VLAN if VLAN configcontrol is set to automatic and that port will then be without VLAN membership. **Workaround**: To reactivate the port, add the port to the desired VLAN and re-enable STP participation for that port as appropriate.

Reference Number	Description
wi00888620	**Brouter Ports**: Avaya recommends that you do not renumber units if brouter ports are used. This may result in routes being improperly deactivated and in loss of connectivity. **Workaround**: If it is necessary to renumber the stack, you should remove brouter ports, renumber the stack and then recreate brouter ports.
wi00944306	**Brouter Port, MSTP**: If you attempt to configure a brouter port on a port which is assigned to a VLAN configured in MSTI when running in MSTP mode, then the operation will not be applied. **Workaround**: If using MSTP mode, move the port to a VLAN which is a member of CIST then perform the brouter port assignment.
wi00949343	**Brouter Port, STP**: By design, STP participation is disabled when a brouter port is configured. If you then delete the brouter port, STP participation remains disabled on that port. **Workaround**: Re-enable spanning tree on the port if required after a brouter port instance is deleted.
wi00946493	**DHCP Snooping Option 82**: When DHCP Snooping is configured with Option 82 support and both the DHCP server (trusted port) and the DHCP client are on the base unit of a stack, then the option 82 information will not be added to the DHCP release packet or the DHCP unicast requests that the client generates. **Workaround**: Locate the DHCP server or trusted uplink ports on a port which is not on the base unit.
wi00949406	**ECMP, Route Display**: When ECMP is configured there may be a discrepancy noted between the routes shown by the **`show ip route`** and the **`show ip num-routes`** commands. This is because the **`show ip num-routes`** command displays routes based on the number of destinations regardless of the number of equal cost paths to that network when ECMP is used. The **`show ip route`** command correctly displays the total number of routes taking into consideration the equal cost paths when ECMP is used.
wi00939421	**EDM, IP Phone Automatic PoE Changes**: When IP Phone Automatic PoE Changes is enabled, the dynamic power limit or dynamic power priority is not displayed in EDM. **Workaround**: Use ACLI to query PoE priority and limits when IP Phone Automatic PoE is configured.
wi00958436	**EDM, MAC Address Table**: When you view the MAC address table from EDM and you request a refresh before the table finishes displaying, the rows from the table may scroll continuously. **Workaround**: If using EDM, wait for the MAC address table to be completely displayed before pressing the refresh button or use the ACLI **`show mac-address-table`** command.
wi00928161	**EDM, PoE Status**: In EDM PoE ports may display an incorrect status of `otherFault` instead of `Deny Low Priority`. **Workaround**: Use ACLI to display the correct PoE status information

Reference Number	Description
wi00949529	**EDM, SFP**: In some cases when a SFP device has been installed in the SFP port of a base in a stack it will not be displayed as being present in EDM. **Workaround**: After a SFP device has been installed you should perform a device refresh in EDM so that the SFP is correctly displayed.
wi00939773	**EDM, SFTP**: If you use SFTP with password authentication enabled and you do not configure a password, no warning message will be generated by EDM and the SFTP operation will fail. **Workaround**: Ensure that you configure a password in EDM for SFTP if the SFTP authentication type is set to password.
wi00896456	**ERS 4800, 4500-PWR+**: When you add an ERS 4800 or 4500-PWR+ unit to an existing stack, that stack must be running 5.6.0 or later release software. If the stack is running an earlier software release, the switch will not be allowed to join the stack as the software on these new models cannot be downgraded to releases prior to 5.6.0. **Workaround**: First upgrade the existing stack to the 5.6.0 or later software. Then add the ERS 4800 or 4500-PWR+ unit to the stack. Alternatively you could add the ERS 4800 or 4500-PWR+ unit as the new base unit to the stack; remembering only one unit in the stack can have the Base Unit switch set to on.
wi00897184, wi00897383	**ERS 4800, Port Statistics**: On ERS 4800 models the port statistics for ifOutDiscards and ipInDiscards are not incremented.
wi00960581	**ERS 4800, RADIUS Management Logging**: When a telnet connection is made to ERS 4800 switch operating in standalone mode, the RADIUS accounting packets sent by the switch will have the NAS-Type-Port attribute incorrectly set to Async rather than Ethernet.
wi00928249, wi00928260	**ERS 4800, Stack Statistics**: On ERS 4800 models the multicast or broadcast packet statistics are not incremented for the **`show stack port-statistics`** command output.
wi00945097	**ERS 4800, TDR**: When performing the TDR function on an ERS 4800 switch, the switch will incorrectly report swapped pairs for a straight through cable.
wi00945147	**ERS 4800, TDR**: When performing the TDR function on an ERS 4800 switch, if the switch is connected to an ERS 4500, then the switch will incorrectly report that pairs 1 and 4 are inverted.
wi00936995	**IGMPv3**: If the size of the IGMPv3 membership report is greater than 1600 bytes, the membership report will not be processed by the switch. IGMPv3 membership reports may contain join requests for multiple groups in one request. **Workaround**: Limit the maximum number of multicast groups per join request to less than 195 groups.
wi00959759	**IGMPv3, Maximum Entries** : The maximum number of IGMP groups learned by IGMP Snooping on the switch is 512. However, this depends on the hardware table usage. With IGMPv1/v2 there is a direct

Reference Number	Description
	correlation between the number of groups and entries. IGMPv3 on the other hand may use more than one hardware entry per group. An IGMPv3 group with N source addresses will typically consume N+1 hardware entries. As an example an IGMPv3 group with 2 specified source will use 3 hardware entries.

wi00861551	**IGMP, Mrouter ports**: With this release IGMPv3 support has been added to the ERS 4000 product. Multicast Router (Mrouter) ports should now be configured under the ip igmp context. Following are some example ACLI commands:
	`ERS4000 (config)# interface vlan 1`
	`ERS4000 (config-if)# ip igmp router 1/4`
	`ERS4000 # show ip igmp snooping`

wi00894579	**IGMP, Multicast Flood, OSPF**: If you configure IGMP Snooping with the unknown multicast no flood option, the system drops control traffic for protocols that use multicasting (example, OSPF). **Workaround**: Configure unknown multicast allow flood specifically for the required multicast group.
wi00934177	**IP Phone Automatic PoE Changes**: If an automatic power limit is configured lower than the static power port limit and is lower than the IP phone power consumption, then the port will cycle through detecting, delivering and overload power states. This is expected operation as the switch will first power up the device as a normal PD. Then once the end device is powered up, the switch will detect the end device as an IP Phone, at which point the automatic power limit will be applied. If the automatic power limit is less than the power being drawn by the IP Phone, then the port will enter an overload state. Once the port enters an overload state, power will no longer be supplied and the IP Phone will power down. After a period of time the switch will again restart power discovery on the port and power up the end device. **Workaround**: Avaya recommends if using IP Phone Automatic PoE that the automatic power limit is set greater than any IP Phone power consumption.
wi00934434	**IP Phone Automatic PoE Changes, Energy Saver**: If Energy Saver has been configured for PoE power savings mode, then it will not take into account the dynamic PoE priority of a port which is allocated through the IP Phone Automatic PoE function. Thus if the underlying static PoE priority is low and even though the IP Phone Automatic PoE has set a port to high or critical PoE priority, energy saver will power down the port if poe-saver is enabled when energy saver activates. **Workaround**: Avaya recommends not to use poe-savings mode in combination with IP Phone Automatic PoE changes with this release.
wi00929526	**IP Routing, Route Summary Display**: When performing the **`show ip route summary`** command, the number of connected routes is incorrectly displayed as 0. **Workaround**: Use the command **`show ip route`** and if necessary perform a count of the directly connected routes.

Reference Number	Description
wi00894103	**NTP**: You can enable NTP without configuring an NTP server, which will result in no time synchronization. **Workaround**: You should configure at least one NTP server for synchronization to occur.
wi00895539	**NTP, IPv6**: NTP does not support the configuration of servers using IPv6 addressing with this release.
wi00934809	**MAC Address Table, Layer 2 FDB**: With the introduction of new features such as static MAC addresses with this release, the MAC addresses of each of the units in the stack will now be shown in the MAC Address table or Layer 2 Forwarding Database (FDB). This is an expected operation and no action is required on your part.
wi00954477, wi00955665	**MAC Address Table, Layer 2 FDB**: With the introduction of new features such as static MAC addresses with this release, the MAC addresses associated with VLAN IDs used by STGs (4001–4008) will now be shown in the MAC Address table or Layer 2 Forwarding Database (FDB). This is an expected operation and no action is required on your part
wi00950703	**Management IP Address, bootp-when-needed, dhcp-when-needed**: If the switch is configured to use `bootp-when-needed` or `dhcp-when-needed` for the management IP address, you may not be able to change the IP address for up to 3 minutes after the agent code becomes operational. **Workaround**: Avaya recommends that you wait approximately 3 minutes after the switch has become operational to change the switch IP address.
wi00961473	**Multicast Traffic, Stack of Two**: When you fail one of the stack cables between a stack of two units, then the multicast traffic matching the rule installed by the **`vlan igmp unknown-mcast-allow-flood`** command (for example to match OSPF hello packets) will be doubled if the egress port is on the other unit in the stack of two. This only occurs on ERS 4800 units and ERS 4500 units with a single ASIC when operating in a stack of 2 units.
wi00962297	**PoE+ Firmware**: In some cases it may be necessary to upgrade the PoE + firmware on PWR+ models. In some cases if you attempt to perform a PoE+ firmware update on a stack of 8 units, the update may fail. The download will always succeed if there are 7 or less PWR+ units in a stack. **Workaround**: Reset the stack and attempt to reload the PoE+ firmware or remove one unit from the stack and re-download the PoE+ firmware.
wi00933497	**Port Mirroring, Ingress & Egress Mirroring**: When you use port mirroring, if a packet is both ingress and egress mirrored, two copies of the packet will be sent to the MTP ports. If the egress port is operating in tagged mode, then one copy of the packet will be untagged and another copy of the packet tagged from the egress port. This is expected operation.

Reference Number	Description
wi00955218	**Port Mirroring, XrxYtx, IP Routing**: When performing port mirroring in XrxYtx mode on an ERS 4500 switch, traffic which is to be routed will not be mirrored; this is a hardware limitation. When performing port mirroring in XrxYtx mode on an ERS 4800 switch, traffic which is to be routed will be correctly mirrored to the mirror to port.
wi00932268	**Port Statistics**: In some situations when a port receives oversized and bad CRC packets or undersized and bad CRC packets the appropriate counters are not correctly incremented.
wi00950622	**QoS, Queue Shaping**: If queue shaping min rate is configured on the highest queue number, then in an oversubscription scenario this rate may not be fully respected if it exceeds 98% from egress bandwidth.
wi00958103	**QoS, Strict Priority, WRR Algorithm**: The ERS 4800 will process traffic differently to ERS 4500 switches when egress queues are congested. On an ERS 4800 switch, during periods of congestion, low drop precedence traffic will be buffered, while high drop precedence traffic could be dropped if there is insufficient egress buffers available
wi00939391, wi00939393	**Shared Port, SFP**: New shared port functionality using the **`shared-port auto-select`** command may not work correctly on models other than the 4526GTX, 4526GTX-PWR, 4548GT and 4548GT-PWR.
wi00959035	**SFP, Display**: If AA14190040 or AA1419029 CWDM SFPs with the vendor ID of OCP are installed in the switch, a **`show interfaces`** or **`show gbic-info`** will incorrectly display these devices as operating at 100Mbps instead of 1Gbps.
wi00927762	**SFTP, Download**: If you use specify an incorrect IP address when you download files from a SFTP server, the system displays an incorrect warning message as follows:`% Tftp server IP address invalid.`
wi00960742	**SNTP, NTP**: You should only configure SNTP, NTP or clock commands via EDM, telnet, SSH or a console port connected to the Base Unit (BU) in a stack. **Workaround**: Avaya recommends for all operations that you should only use a console connected to the base unit of a stack.
wi00859047	**SSH**: The CLI command **`show ssh download-auth-key`** does not display the last transfer result when you download the key from USB. **Workaround**: If the download of the SSH key was successful, then when you display the ssh or sshc status you will see the key has been loaded by the switch. Alternatively loading the SSH key from a TFTP server will display the correct result.
wi00959582	**SSH, DSA/RSA Key Length**: When you upload the DSA/RSA key to a TFTP server or USB device from a switch/stack you can generate a filename with up to 128 characters. When you attempt to download the DSA/RSA keys, the switch supports a maximum of only 30 character filenames. **Workaround**: Avaya recommends you use filenames with a maximum of 30 characters for DSA/RSA keys.

Reference Number	Description
wi00891090	**SSH Client, Break Sequence, Syslog**: When you use the SSH client from the switch or stack, if you terminate a server connection with the "~." break sequence, the system does not generate a `SSH disconnected` syslog message.
wi00961775	**Upgrade to 5.5 or 5.6, RADIUS Password Fallback**: When upgrading to Release 5.5.x or 5.6.0, the RADIUS Password Fallback setting will become disabled during the upgrade process. This does not occur if upgrading from 5.5.x to 5.6 or later releases. If RADIUS Password Fallback becomes disabled, login access to the switch may be impacted if the RADIUS server becomes unreachable. **Workaround**: Before commencing the software upgrade from releases prior to 5.5 to release 5.5 or 5.6 if you are using RADIUS fallback, set the password authentication to local; perform the software upgrade; then login to the switch using the local password; then re-enable RADIUS password and RADIUS fallback.
wi00961795	**Upgrade to 5.6, IGMP, Unknown Multicast Allow**: When upgrading to Release 5.6 or later, any previously configured Unknown Multicast Allow flood addresses will be lost. This is a result of the change to multicast support in the 5.6 Release. **Workaround**: In previous software releases, the list of addresses was a global setting. Following an upgrade, you must configure the allow flood addresses on a per VLAN basis.
wi00894057	**Voice VLAN, 802.1AB (LLDP)** : When you can create a LLDP MED network policy there is no check performed to ensure that the VLAN type is set to Voice. **Workaround**: Ensure that you configure the VLAN appropriately as a Voice VLAN before setting the LLDP MED network policy.
wi00893827	**Voice VLAN, ADAC, EAP**: Avaya recommends you do not use the same VLAN ID for ADAC Voice VLAN and EAP Voice VLAN.
wi00930645	**Voice VLAN, 802.1AB (LLDP) MED Policy**: When you configure a VLAN as type Voice, you will still need to explicitly configure 802.1AB (LLDP) MED Network policy to advertise that VLAN via LLDP to end devices.

Known Issues and Limitations for Releases Prior to Release 5.6

The following section lists known issues and limitations in Avaya Ethernet Routing Switch 4000 Series software which are present in Release 5.6 and are also known to be present in older releases of the software.

Table 11: Known issues and limitations

Reference number	Description
wi00868382, wi00554875	**802.1AB / LLDP Default Parameters, ADAC**: In Software Release 5.5, 5.6 and later with the introduction of 802.1AB default parameters a default LLDP MED policy is configured on all ports. The default values for that policy are as follows: application type = voice, tagging = untagged, DSCP = 46 and VLAN priority = 6, VLAN id= 0. If ADAC is configured on that port and an IP Phone is detected, the dynamic LLDP MED policy will not be installed, resulting in the IP phone not receiving the correct VLAN configuration if ADAC tagged frames is used. This happens because the default MED policy is static and overrides the dynamic policy installed by ADAC. **Recommendation**: If ADAC is to be used, then it is recommended that the default 802.1AB/LLDP MED policies are deleted on telephony ports and on uplink/call server ports. Use the interface command `no lldp med-network-policies` on telephony ports and on uplink/call server, prior to configuring ADAC on ports.
wi00863027	**802.1AB Default Values**: When you upgrade to 5.5 or 5.6 software, any old 802.1AB values will be maintained. The new default 802.1AB values are only applied if you reset the configuration (for example, use the `boot default` command).
wi00856869	**802.1AB Integration / ADAC**: Avaya IP Phones will perform a reset when connecting to the switch if 802.1AB Integration (use of 802.1AB TLVs) is enabled in conjunction with ADAC. **Workaround**: Create a manual 802.1AB-MED network policy which will then change the order in which information is supplied to the IP Phones.
wi00857043	**802.1AB Integration / Avaya 1100**: Avaya 1100E IP Phones using firmware SIP1120e04.00.04.00 will not be recognized by the 802.1AB integration capabilities of the switch, as these phones use the manufacturer name in the TIA-Tx-TLV of "Avaya-01" which is different from the expected value of "Avaya". **Workaround**: Avaya 1100 IP Phones can be configured via alternative means such as DHCP.
wi00858022	**802.1AB Integration / Avaya IP Phone**: When the switch detects an Avaya IP Phone, it sends four LLDP packets (according to MedFastStartRepeatCount). With some models of Avaya IP Phone, this process is repeated 60 seconds after device detection. **Workaround**: None required.
wi00861373	**802.1AB Integration / Call Server TLV**: An IP Phone may incorrectly report the Call Server in-use IP address to the switch if different call-servers were previously configured and cached by the IP Phone. **Workaround**: If it is found that there is a mismatch of in-use call-server addresses cached by the IP Phone, then performing two consecutive resets of the IP Phone will clear the incorrect data from the IP Phone cache and result in correct information being returned to the switch.
wi00861372	**802.1AB Integration / Call Server TLV**: You can configure up to 8 Call Server IP Addresses on the switch for maximum resiliency. When

Reference number	Description
	some of the Call Servers are unreachable, the Avaya IP Phone may incorrectly indicate to the switch that it is using one of the unreachable Call Servers. **Workaround**: Information on call server use can be obtained from the phone or the call server.
wi00849008	**802.1AB Integration / dot1q-framing TLV**: When Avaya proprietary TLV dot1q-framing is set to auto, the IP Phone will always use untagged mode, irrespective of MED Network Policy or other setting being present. **Workaround**: It is recommended not to use the dot1q-framing TLV set to auto, but instead to set the mode to tagged or untagged.
wi00859649, wi00859648	**802.1AB Integration / File Server TLV**: The File Server IP Address which the IP Phone is using is not advertised by some Avaya IP Handsets (9630, 9620L, 9630G, 9640, 9620C) back to the switch. This can result in the switch displaying null information as the configured file server for these IP phones. **Workaround**: Information on fileserver use can be obtained from the phone or call server.
wi00862047	**802.1AB Integration / Phone IP TLV**: If the Avaya IP Phone receives its IP Address from a DHCP server then the 802.1AB TLV message from the IP Phone to the switch will not contain the IP Address of the phone, but will only contain the gateway address and netmask.
wi00855665	**802.1AB Integration / Phone IP TLV**: The gateway address returned by an Avaya IP Phone in the IP Phone TLV will be null until the IP Phone is able to reach the configured File Server. Once the IP Phone has reached the File Server, then the correct gateway address will be advertised in this TLV and displayed by the switch. **Workaround**: This does not result in any operational issues which require a workaround.
wi00850597, wi00850033, wi00850936, wi00850590, wi00850935	**802.1AB Integration / Power Conservation**: If the switch sets the power conservation TLV to zero (indicating that no power conservation should be used by the IP Phone), Avaya 9600 IP Phones will always return a value of 1. **Workaround**:This does not result in any operational issues which require a workaround.
wi00855650	**802.1AB Integration / SIP Configuration**: The currently defined Avaya Proprietary TLVs, do not support the direct provisioning of SIP parameters (transport protocol, port number, domain name) from the switch to the IP Handset. **Workaround**: The SIP information can be supplied to the IP Phone through the configuration file server, ensure that the File Server TLV is appropriately configured.
wi00862943	**802.1AB Integration / VLAN Name TLV**: Avaya IP Phone does not use information from 802.1AB VLAN Name TLV to configure Voice VLAN. Other devices will correctly set the Voice VLAN if the VLAN name is set to voice.
wi00865086, wi00954114	**Avaya IP Phone DHCP Option 242, 802.1AB (LLDP) Default Parameters**: If you have configured Avaya IP Phones with DHCP Option 242 to specify the Voice VLAN (L2QVLAN) the IP Phone will

Reference number	Description
	not use the correct VLAN if the switch is using the 802.1AB (LLDP) Default Parameters. Also refer to wi00868382, wi00554875 **Workaround**: If Avaya IP Phones with DHCP Option 242 are to be used, then it is recommended that the default 802.1AB/LLDP MED policies are deleted. Use the interface command **`no lldp med-network-policies`** on telephony ports.
wi00841065	**802.1AB MED Network Policy**: When upgrading to 5.5 or 5.6 software and the previous configuration contained no network policies, the new default network policies will be applied.
wi00841955	**802.1AB MED, Auto QoS**: Having a custom LLDP MED policy and enabling Auto QoS will result in the LLDP MED network policy being saved with a DSCP value of 47.
wi00862054	**802.1AB VLAN Name TLV**: When the command **`lldp tx-tlv dot1 port-protocol-vlan-id vlan-name`** is issued on an interface, an incorrect error message `Port(s) not members of all VLANs configured` may appear. This does not affect functionality of VLAN-name or port-protocol TLV.
wi00484050	**ACG, SNMPv3, Secure Image**: When you run the secure software image, an ASCII configuration file generated by the switch has the SNMPv3 user commands **`snmp-server user`** commented out. This is expected behavior as the associated passwords cannot be output in clear text in the ASCII generated file due to security requirements. As a result when the configuration is loaded onto a switch with default configuration, the SNMPv3 users are not recreated. **Workaround**: Manually recreate the SNMPv3 users after loading the ASCII configuration.
wi00491471	**ADAC, EAP, Guest VLAN**: If you configure both Guest VLAN (GVLAN) and ADAC untagged frames advanced mode on a port, then when a device is discovered by ADAC the port is moved from the GVLAN into the ADAC Voice VLAN. This results in lost connectivity for the GVLAN. If you disable ADAC globally, the client is removed from the ADAC Voice VLAN and placed in the initial port based VLAN with the PVID set to 1 (the default VLAN). **Workaround**: Avaya recommends you do not use ADAC untagged frames advanced mode in combination with EAP MHMA and Guest VLAN.
wi00491178	**CPU utilization**: The CPU utilization reported for the 'last 10 minute interval' may be higher than actual if the CPU was loaded at 100% for the first 5 minutes then returns to an idle state for the next 5 minutes. All other values are correctly calculated. The value will be properly displayed after 30 minutes if the CPU load returns to normal activity levels.
wi00951324	**DHCP Snooping External Save, Replacing Base Unit**: If you replace the Base Unit (BU) in a stack, the filename used for DHCP Snooping External Save will no longer be valid. **Workaround**:

Reference number	Description
	Reconfigure the DHCP Snooping External Save filename after replacing the BU in a stack.
wi00880382, wi00891087	**DHCP Snooping External Save, Transition to Standalone**: If DHCP Snooping External Save is configured to use a USB port on a unit in the stack and then the stack is transitioned to standalone operation, the applicable USB unit number and filename information will become invalid. **Workaround**: Re-configure the filename settings for operation once the switch is operating in standalone mode or configure DHCP Snooping External Save to use the USB ports on the unit which is to become the standalone unit.
wi00932189	**DHCP Snooping External Save, USB, Stack Renumbering**: If you have DHCP Snooping External Save configured to save the database to a USB drive on a particular unit, then if you perform a stack renumbering the feature may incorrectly point to the USB device on the wrong unit. **Workaround**: If you have DHCP Snooping External Save configured to save the database to a USB drive, then after performing a stack renumbering you should re-configure DHCP Snooping External Save to use the renumbered unit in which the USB devices is located.
wi00484170	**EAP, 384 ports, Intruder MAC**: If you enable or activate EAP on 384 ports simultaneously, while all clients are sending large volumes of traffic, then some intruder (unauthorized) MAC addresses may not appear in the MAC address table. This applies only to intruder addresses which are blocked and not allowed to forward traffic and it is not a security or connectivity problem.
Q01981920	**EAP, Fail Open VLAN**: An EAP or Non-EAP client could be assigned to the Fail Open VLAN in normal operation if the VLAN name or ID returned from the RADIUS server matches the VLAN assigned for the Fail Open VLAN. **Workaround**: Ensure that the Fail Open VLAN name or ID that you use does not match one of the returned RADIUS VLANs.
wi00490753	**EAP, Fail Open VLAN**: When a device is moved into or out of the Fail Open VLAN, there is no notification to the end client that the VLAN has been changed. **Workaround**: It is recommended that if Fail Open VLAN is used, you should set the DHCP lease time to a short period so that clients regularly refresh their IP address leases. Alternatively, if a client has been moved to the Fail Open VLAN, then issuing a DHCP release and renew on the client obtains a new IP address appropriate for the Fail Open VLAN.
wi00491652	**EAP, Guest VLAN**: If you disable Guest VLAN (GVLAN) globally or per interface while authenticated clients are present, the system does not remove the port from the GVLAN. **Workaround**: It is recommended that you shut down the switch port before you disable GVLAN, either globally or per interface. Shutting down the port clears the authenticated clients so that the ports are correctly removed from the GVLAN.

Reference number	Description
wi00484217	**EAP, MHMA MultiVLAN, Guest VLAN** : Switch ports are not moved into the Guest VLAN (GVLAN) if you enable the GVLAN option after EAP clients have authenticated on the port. **Workaround**: It is recommended that you enable Guest VLAN (global or per port option) before EAP clients are authenticated. Alternatively, you can globally disable EAP, configure GVLAN, then re-enable EAP globally.
wi00878611	**EAP, NEAP, Fail Open VLAN**: After the RADIUS server becomes unreachable, then reachable again, not all 384 NEAP clients may be re-authenticated in some circumstances. **Workaround**: After the RADIUS server becomes reachable, you can either reboot the stack or manually clear the MAC address table on the EAP enabled ports using the interface configuration command **`clear mac-address-table interface fastEthernet <portlist>`**.
wi00491727	**EAP, QoS Traffic Profiles**: If you configure both QoS Traffic Profiles and EAP, in some circumstances after a switch reboot the QoS Traffic Profile may be set to a higher precedence than before the switch reboot. EAP packets could then be blocked by rules defined in the traffic profile. **Workaround**: To prevent EAP packet blocking in this situation, you can define a QoS policy instead of using a Traffic Profile. The same filtering capabilities are supported, but user defined policies use the same QoS precedence correctly before and after a reset.
wi00483818	**EAP, RADIUS Last Assigned VLAN**: When a port is configured for RADIUS Last Assigned VLAN, if the last RADIUS authentication for that port does not contain QoS priority, then the port priority will be either the one manually configured for that port or the one received for the previous authenticated client.
wi00483930	**EAP**: When EAP performs authentication through TTLS, the first authentication between the supplicant and the switch may fail but subsequent authentications will succeed. **Workaround**: If authentication fails when using EAP-TTLS, do one of the following: • Wait 30 seconds for the client to re-authenticate successfully • Use an alternative EAP authentication mechanism for the client
wi00944065	**EDM, 802.1AB (LLDP) dot1**: When displaying 802.1AB (LLDP) 802.1 parameters in EDM, the switch configured parameters are not displayed in the Local Protocol VLAN and Local VLAN Name tabs.
wi00489861	**EDM, ASCII Configuration**: When loading an ASCII configuration file using EDM it is recommended that the switch has minimal configuration changes from default. Otherwise existing switch/stack configuration might cause warning or error messages that force the ASCII configuration to exit with a FAIL status. **Workaround**: Apply ASCII configuration from EDM to a switch or stack that has a basic configuration. Alternatively, a currently-configured switch/stack can be re-configured using an ASCII configuration via CLI (console, telnet,

Reference number	Description
	SSH) since the system ignores warning and error messages and configuration continues until the last ASCII file line executes.
wi00906624	**EDM Help, Classifier Blocks**: The EDM help text for QoS Classifier Blocks incorrectly states that the eval order parameter can range from 0 to 65,535 when it should state 1 to 65,535.
wi00893619	**EDM, Firefox, Ipmgr blocked**: When you open EDM in Firefox on a switch/stack where the ip manager has blocked the source IP address of your browser, you will get a blank page in the Firefox browser rather than a pop-up box advising that access from your browser IP address is blocked. **Workaround**: Using IE will result in the appropriate pop-up box advising that access from your browser IP address is blocked.
wi00962126	**EDM, Memory Utilization**: The Memory utilization information which is shown in EDM may not reflect the correct values. **Workaround**: Use ACLI or SNMP to obtain the correct values.
wi00491403	**EDM, Multiport configuration**: When you use EDM to apply an operation to all ports, the system may generate a misleading error message if the change could not be applied to all ports (for example if applying a PoE setting to PoE and non-PoE ports). EDM provides only an error message indicating the first port for which it was unable to apply the configuration change.
wi00950722	**EDM, QoS, Traffic Profile Classifier**: If you use EDM to create a traffic profile classifier, it will be created with an invalid burst-size of 0 unless you also configure metering. This will result in a classifier which cannot be applied. **Workaround**: When using EDM to create a traffic profile classifier always configure a metering value. Alternatively use ACLI to create a traffic profile classifier.
wi00950753	**EDM, QoS, Traffic Profile Committed Rate**: If you configure a Traffic Profile Committed Rate in EDM, the value configured and saved by the switch will be less. **Workaround**: Use ACLI to configure Traffic Profile Committed Rates.
wi00907795	**EDM, RMON Alarms**: When you use EDM to configure alarms for RMON Statistics variables you need to set the interface index manually. The interface index is calculated as index = port number + (64 * (unit number -1)). For example port 2/48 is 48 + (64 * (2-1)) = 112.
wi00876311, wi00897706	**EDM, Script Busy**: When connecting to EDM the following message may appear: `A script on this page may be busy, or it may have stopped responding. You can stop the script now, or you can continue to see if the script will complete`. **Workaround**: Check the remember option and click the continue button from the browser and the message will no longer be displayed.

Reference number	Description
wi00841212. wi00483820	**EDM, TACACS+**: You cannot use EDM to enable TACACS+ because the system disables Web access to the switch when you enable TACACS+ via EDM. If you used EDM to enable TACACS+ you would lose EDM access for any subsequent operations.
wi00930313	**EDM, USB, Binary Configuration**: When saving a binary configuration file to a USB device, if you do not specify a Binary Config Filename, the following message is displayed which may be misleading: `No USB storage device detected`. **Workaround**: Set the binary config filename in order to save/retrieve the configuration to/from a USB device.
wi00846698	**EDM**: EDM multiport select does not work on interfaces with SFPs/ XFPs inserted. Please use per port configuration for interfaces with optics installed.
wi00554891	**EDM**: If the browser device has multiple active IP addresses, EDM will only support multiple sessions from the same source IP address on the device. If different IP source addresses are used, the second or subsequent browsers will display the error message `503 Server Busy`. **Workaround**: If you require multiple EDM sessions from the same client device which has multiple IP interfaces, ensure the Web browser on the device uses the same source IP address.
Q02121888, Q02121890	**Energy Saver, Copper ports, RIP, OSPF**: When you activate or deactivate energy saver, the link on a port briefly transitions. This transition may cause OSPF neighbor connectivity to bounce or cause relearning of RIP routes. **Workaround**: Avaya recommends that you disable energy saver on copper uplink ports which have OSPF adjacencies or RIP routes active. Copper ports, OSPF adjacencies—If you use copper ports for which energy saver is enabled and OSPF adjacencies are exchanged over these links, you can set the ip ospf advertise-when-down enable parameter so that adjacencies are not bounced when the link transitions. Copper ports, RIP routes—If you use copper ports for which energy saver is enabled and RIP routes are exchanged over these links, you can set the ip rip advertise-when-down enable parameter so that RIP routes are not bounced when the link transitions. Alternative: If you use fiber ports for OSPF adjacencies or RIP route connections, energy saver will not cause a link transition.
wi00928532, wi00930048	**Energy Saver, PoE Savings**: If Energy Saver is active and the switch or stack is reset, then the PoE savings will be reported as zero until Energy Saver goes through another activation cycle. This is normal operation as the switch needs to be operating in non-Energy Saver mode first to determine how much PoE is being saved when Energy Saver activates.
wi00900252	**Energy Saver**: If you disable Avaya Energy Saver while it is in power saving mode on ports which are administratively set to 100Mbps, these ports will then operate at 10Mbps. **Workaround**: Deactivate

Reference number	Description
	energy saver using the **`energy-saver deactivate`** command in Privileged EXEC mode before disabling energy saver.
wi00483987, wi00484314, wi00484346, wi00491683	**Energy Saver**: When energy saver is activated or deactivated, the link on a port transitions briefly. This brief transition can cause some devices to reacquire connectivity, but, in most situations, end users do not notice the port transition. On the switch, the system clears the MAC address for the port and then relearns it. If EAP or NEAP is enabled, EAP authentication restarts. **Workaround**: Avaya recommends that you disable energy saver on copper uplink ports because activating or deactivating energy saver on copper ports triggers a link down followed rapidly by a link up event. Alternative: Use fiber ports for uplinks because energy saver does not change fiber port status when energy saver is activated or deactivated
wi00931011	**IP Source Guard (IPSG), MLT, DMLT, LAGs**: If IPSG is configured on MLT/DMLT/LAG/DLAG ports and these ports are manually shutdown, then entries may remain in the IPSG filtering table even though there are no longer any addresses associated with the port. **Workaround**: Avaya recommends that if trunk ports are likely to be regularly manually shutdown and enabled, that IPSG should not be configured on trunk ports (MLTDMLT/LAGs).
wi00490844	**IP Source Guard (IPSG), Traps**: If the maximum IP entries have been learnt on a MLT/LACP enabled port, then if that trunk is disabled additional log messages are generated.
Q01979384	**IPv6**: Due to the short, or transient, nature of TCP connections for HTTP requests it is likely that IPv6 HTTP connections may not be displayed when you use the CLI command **`show ipv6 tcp connections`**. This behavior is considered normal. **Workaround**: If simultaneous Web page refresh commands are issued, then a **`show ipv6 tcp connections`** command displays the active TCP connections for the Web session.
wi00489936	**Jumbo Frames**: As the Avaya Ethernet Routing Switch 4000 supports jumbo frames (up to 9216), the Jabber counter will always be displayed as zero (0). **Workaround**: You can find information about framing errors in the etherStatsCRCAlignErrors counter.
wi00489794	**Link-up during boot**: During reboot or power up operations, but before the agent code loads, the switch may provide an intermittent link to devices connected to front panel ports. Regardless, no traffic switching occurs until the agent code load completes. **Workaround**: If uplinks are connected to fibre SFP/XFP/SFP+ devices then these devices will not provide link-up until the switch is fully operational.
wi00952359	**LACP, 802.3ad**: When you reboot a switch/stack, the LACP trunk numbers are assigned according to the order in which the trunks are established with neighbor LACP devices. This is normal operation.

Reference number	Description
wi00930449	**MAC Security, MLT, DMLT, LAGs**: Traffic may be incorrectly filtered if MAC security is enabled on trunk ports. **Workaround**: MAC security should not be configured on trunk ports (MLTDMLT/LAGs).
wi00961451	**MAC Security, s5SbsViolationPortIndx**: When MAC Security is enabled and an intrusion occurs, the s5SbsViolationPortIndx MIB object incorrectly reports the real port index. **Workaround**: To calculate the port index on which the intrusion event occurred, subtract 1 from the value returned by the port index for the SNMP trap.
wi00930456	**MAC Security, SNMP Traps**: When MAC security is enabled globally, the s5EtrSbsMacAccessViolation trap is disabled. **Workaround**: Enable the trap manually using the **`snmp-server notification-control s5EtrSbsMacAccessViolation`** command.
wi00483597	**Management VLAN**: When operating in Layer 3 mode, using the Management VLAN for normal routing may result in lost connectivity to the Management IP address. **Workaround**: If connectivity problems occur to the management IP address, clear the ARP cache.
Q02118229	**MIB, EAP, MHMA MultiVLAN**: If you disable the MHMA MultiVLAN option, the SNMP MIB object (bseeMultiHostStatusVid) that reports the VLAN associated with a client reports a value of either 4095 or 4096. The returned VLAN ID values of 4095 or 4096 indicate that the VLAN was not assigned to the client. This is normal, expected behavior in this scenario. Use the CLI command **`show eapol multihost status`** to confirm the VLAN ID association.
wi00848300	**NEAP, IP Phone, Multi-VLAN, ADAC**: If EAP Voice VLAN is used in combination with non-eap-phone option and ADAC is configured for tagged frames and EAP multi-vlan is enabled; then if EAP is disabled after IP Phone is detected and authenticated the PVID of the port is reset to the initial value instead of remaining equal to the value set by ADAC. **Workaround**: Perform a poe shutdown and then no poe shutdown on the IP Phone port so that the Phone is rediscovered and the PVID is set accordingly.
wi00863853	**NEAP, Multiple Requests:** If the switch is operating with more than 1 NEAP client per port and you issue the **`clear mac-address-table`** or **`clear eapol non-eap`** command, then the switch sends multiple consecutive access-request for the same NEAP client, during the same authentication session.
wi00483323	**NSNA**: After rebooting a switch or stack with NSNA MAC based clients connected, the switch may incorrectly report that the devices are in the RED VLAN even though they are actually in the Green VLAN. **Workaround**: Execute the CLI commands **`shutdown`**, then **`no shutdown`** on the corresponding ports.

Reference number	Description
wi00490890	**NSNA**: After units are rebooted in an operational stack, some static MAC authentication clients may be incorrectly displayed as a 0.0.0.0 IP address instead of the correct IP address. This is a display issue only and does not affect functionality. **Workaround**: Use the SNAS to show the correct IP associations.
wi00483205	**NSNA**: For a MAC authenticated client, if the MAC address is deleted from the SNAS database, the SNAS does not send a reset event to the switch, so the client will remain in its currently assigned VLAN. **Workaround**: Execute ACLI commands **`shutdown`**, then **`no shutdown`** on the corresponding ports.
wi00483629	**NSNA**: If you add a new classifier to the NSNA yellow QoS set (exceeding the resources), the yellow filters may not be applied.
wi00491369	**NSNA, DHCP Snooping, Dynamic ARP Inspection (DAI)**: If NSNA trusted port is set in combination with DHCP Snooping and Dynamic ARP Inspection (DAI), then occasionally, after a switch reboot, some PCs connected to the switch may be unable to correctly reacquire an IP address and will appear in the **`show nsna client`** command with an IP address of 0.0.0.0. **Workaround**: Disconnect and reconnect the PC, or if using Windows, issue an ipconfig /release and then ipconfig /renew command and the PC will correctly reacquire an IP address.
wi00483355	**Port Mirroring, Bootp**: Due to a hardware limitation, the BOOTP packets cannot be mirrored if the mirror port is on the first ASIC (port 1-24).
wi00900220	**Port Mirroring, XrxYtx**: In XrxYtx port mirroring mode broadcast traffic may not be correctly mirrored to the monitor port.
wi00491450	**Port Mirroring, XrxYtx, XrxYtxOrYrxXtx**: If you use port 1 as a mirror port in XrxYtx or port mirroring modes, then broadcast or multicast traffic mirrored to the port is doubled on the monitor port. **Workaround**: Use another port on the switch as the mirrored port.
wi00870638	**Port Mirroring, XrxorYtx**: When you configure port mirroring in XrxorYtx mode, then STP, LLDP and autotopology packets will be mirrored with VLAN ID 1 on untagged ports, even if the ports are not members of that VLAN.
Q01977243	**QoS information**: Non QoS applications, such as UDP Forwarding and IP Source Guard, should be configured prior to configuration of QoS policies to avoid the potential conflict in filter precedence order which can result when the binary configuration file is reloaded. In some rare cases, when QoS precedence's are configured before non- QoS applications that use filters—for example: UDP Forwarding, NSNA, and IP Source Guard—the QoS information saved in the binary configuration file may not be correctly reloaded to the switch. The greater the number of filter-using non-QoS applications per port, the greater the probability that the QoS information in the binary

Reference number	Description
	configuration file may be reloaded incorrectly. If the QoS information in the binary configuration file is reloaded incorrectly, some of the QoS precedence's may not be configured correctly.
Q02088900	**QoS, information**: The system performs bandwidth allocation for queues according to Strict Priority and WRR algorithm. When you configure shapers on queues with minimum rate, the system first queues traffic to ensure the minimum rate is achieved for all queues. The system then allocates the remaining egress bandwidth according to Strict Priority, WRR and shape maximum rate configured for each queue. In case the sum of shape minimum rates configured (queue shapers) exceeds the line rate, the minimum shape rate is assured for queue 1 and then the remaining bandwidth is distributed amongst the rest of the queues. The system uses the WRR algorithm to best assure that the minimum rates for the rest of the queues are achieved. Note: If you have ERS 4000 and ERS 5600, in the same scenario the ERS 5600 operates differently, depending on the active queue set, and may use strict priority, WRR and RR algorithms.
wi00860958	**RADIUS Accounting**: If RADIUS accounting is enabled and the switch/stack is reset, then the accounting messages sent to the RADIUS server will only include a `RADIUS Accounting Off` message (no `RADIUS Accounting Stop` messages will be sent for authenticated clients).
wi00878635	**RADIUS, EAP Server, NEAP Server, Fail Open VLAN**: While servers are unreachable and ports are in Fail_Open VLAN deletion of all of the RADIUS servers of a given type (e.g. all EAP Servers, all NEAP Servers) may result in clients not being properly re-authenticated or assigned to the appropriate RADIUS VLAN. **Workaround**: Do not delete all RADIUS server types when RADIUS servers are unreachable. Alternatively after the RADIUS servers are again reachable, manually clear the MAC address table on the EAP enabled ports using the interface configuration command **`clear mac-address-table interface fastEthernet <portlist>`**.
wi00864589	**RADIUS, Interim Updates**: After RADIUS accounting is disabled for a RADIUS server, interim updates will still be sent to that server, if they were previously enabled. It is recommended that you turn off interim updates also, if it is desired not to receive them.
wi00490762, wi00483513	**RSTP**: When operating as an RSTP root bridge and the Base Unit in a stack is reset, or the stack transitions to standalone mode, the system may not always generate the SNMP trap message indicating a change in RSTP root. **Workaround**: A local log message for nnRstNewRoot is always generated.
wi00484096	**show running-config**: When you execute the **`show running-config`** or **`show running-config module`** commands the system may take a longer time than expected to display the output. In

Reference number	Description
	systems with very large and complex configurations of 8 units in a stack it can take up to 4 minutes to complete the display of the command. This is considered normal behavior
wi00484079	**SNMP Traps, Temporary Base Unit**: If you create new SNMP Trap notification filters while the stack is operating in Temporary Base Unit (TBU) mode (that is the Base Unit has failed) then the new filters are not saved and are lost upon stack reboot. **Workaround**: If the stack is operating in TBU mode, reset the stack and then create the required SNMP Trap notification filters.
wi00496736	**SNMPv3, ACG**: SNMPv3 user commands (for example, snmp-server user) are commented in the text configuration file generated by the switch or stack if running the SSH version of the switch software. This happens because the associated passwords cannot be put in clear text in the generated configuration file. Please note that when the configuration is loaded the SNMPv3 users are not recreated.
wi00489857	**SONMP**: A change in the operation of the SONMP-based auto topology means that directly connected BayStack 450 switches report a physical auto topology change every 70 seconds to the Avaya ERS 4000 switch. You can ignore this auto topology change message where there is a direct connection from the Avaya ERS 4000 to a BayStack 450 switch.
wi00942683	**Spanning Tree**: When changing the STP mode from STPG to RSTP, or from MSTP to RSTP, the learning on the ports from groups other than group 1 will be set to disabled. **Workaround**: You will need to re-enable STP on other STP groups if so desired after re-configuration of the switch.
wi00862444	**TACACS+, Layer3**: In a layer 3 environment if the management VLAN is not operational (no link is up on that VLAN), the switch does not generate TACACS+ packets, therefore no authentication can be performed against the TACACS+ server. **Workaround**: Ensure that management VLAN is up.
wi00491296	**Telnet, ASCII Config** : If you configure a very short telnet timeout value and then you connect to the switch using telnet to execute the CLI command copy config, to save the ASCII configuration to USB or TFTP, the configuration file may be incomplete for large or complex stack configurations. **Workaround**: It is recommended to set the minimum telnet timeout value to 5 minutes.
wi00491518	**VLACP**: When you disable VLACP globally or on a per interface basis, the system forwards the following incorrect message to the syslog server: `Port X re-enabled by VLACP`.
wi00933290	**VRRP, Management VLAN**: If you create a VRRP interface on the management VLAN, the VRRP information will not be saved in the configuration file. This is operating as intended. **Workaround**: Avaya recommends that VRRP should not be configured on the Management VLAN of the switch/stack.

Reference number	Description
wi00888446	**VRRP**: If VRRP is configured on a VLAN which used the VLAN ID of 4094, then while the configuration took place, show commands will not display this VRRP instance or configuration information. **Workaround**: It is recommended to use VLAN IDs in the range of 1-4093 for VRRP configurations.
wi00863879	**VRRP**: VRRP may become unstable when multiple VRRP instances with Fast Advertisement are enabled. **Workaround**: If a large number of VRRP instances are to be configured, it is recommended that the minimum Fast Advertisement Interval (FAI) is set to no less than 600ms.

IPv6 limitations

The following table lists limitations specific to the implementation of IPv6 in this release.

Table 12: IPv6 limitations

Reference number	Description
1	IPv6 Management should only be configured from a base unit in stack.
2	Only one IPv6 address can be configured and it will be associated to the management VLAN.
3	No DHCP/BOOTP, Stateless Address Autoconfiguration or IPv6 loopback address is supported for the management address.
4	The only IPv4 to IPv6 transition mechanism supported is dual-stack (no tunnelling).

Chapter 7: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.