Avaya Release Notes — Release 5.5 Avaya Ethernet Routing Switch 4500 Series

5.5
NN47205-400, 07.06
May 2011

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 Web sites 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 Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

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 RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 RESELLER; 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”).

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

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: New in this release

The following sections detail what is new in Avaya Ethernet Routing Switch 4500 Series Release Notes — Software Release 5.5.

Features

See the following sections for information about new features.

802.1AB customization

802.1AB, Link Layer Discovery Protocol (LLDP) customization expands LLDP capabilities so that you can customize all of the LLDP advertisements and timers. The enhanced flexibility provided by the additional customization makes LLDP suitable for deployments where a variety of vendor equipment or deployment methods exist.

You can customize the following Type, Length, and Value (TLV) elements for your deployment needs:

- System TLV
- Port Description TLV
- System Name TLV
- System Description TLV
- System Capability TLV
- Management Address TLV
- VLAN Name TLV
- Port VLAN ID TLV
- Port and Protocol VLAN ID TLV
- MAC/PHY configuration/status TLV
- Power via MDI TLV, Link Aggregation TLV
- Maximum Frame Size TLV
- LLDP MED Capabilities TLV
- Network Policy TLV

- Location Identification TLV
- Extended Power-via-MDI TLV and Inventory TLV

You can also configure the following timers:

- Reinitialization Delay
- Transmit Interval
- Transmit Delay
- Transmit Hold
- Fast Start Timers
- LLDP Timers
- SNMP Notification Interval

802.1AB integration

With 802.1 AB, Link Layer Discovery Protocol (LLDP) integration you can simplify the deployment of Avaya voice solutions with Avaya data products because 802.1 AB integration supports a set of Avaya-specific TLVs that you can use to provision and report about parameters that support Avaya IP Telephones. When you use the 802.1AB integration TLVs, you achieve a more rapid deployment of voice solutions and you can also view information from the data network about the services the voice solutions use. 802.1AB integration also works with Avaya Energy Saver to maximize off-peak power savings for network and voice services without impact to service.

802.1X non-EAP Accounting

Accounting support is extended to generate accounting messages and interim updates for non-EAP (NEAP) clients. If you configure different servers for EAP and non-EAP clients, the system directs accounting messages to the appropriate EAP and NEAP servers.

802.1X non-EAP re-authentication

You can use non-EAP (NEAP) re-authentication to resolve connectivity issues that occur when devices authenticated by NEAP enter sleep mode or are decommissioned and removed from the RADIUS database. When you use NEAP to authenticate devices such as printers, IP cameras, and card readers, you can set defined re-authentication intervals so that an idle device does not lose network connection and a decommissioned device does not occupy a connection.

802.1AB new default parameters

Beginning with Release 5.5, you can improve Voice and Video over IP function because some of the LLDP parameters are enabled by default. Now you can connect LLDP enabled IP

handsets to the switch and start deployment without additional configuration. The following LLDP parameters are enabled by default:

- lldp config-notification
- lldp status txAndRx config-notification
- lldp tx-tlv local-mgmt-addr port-desc sys-desc sys-name
- lldp tx-tlv dot3 mdi-power-support
- lldp tx-tlv med extendedPSE inventory location med-capabilities network-policy
- lldp med-network-policies voice dscp 46 priority 6

AUR enhancement

With Automatic Unit Replacement (AUR), you can display a list of all of the MAC Addresses for stack switch units and display whether or not the units are operational. Beginning with Release 5.5, for demonstration or troubleshooting operations, you can remove the MAC Address for a non-operational unit from the AUR address cache. Then, when you insert the unit back into the stack, the stack treats that unit as a replacement unit, rather than an existing unit which has been returned to service. The stack then ensures that the diagnostic and agent software for the unit are the same as that operating on the stack and restores the local configuration data for the re-inserted unit.

DHCP Snooping External Save

You can use DHCP Snooping External Save to automatically save the DHCP Snooping database once every 5 minutes, to a specified external location, such as a TFTP server or USB drive. The switch can then retrieve stored DHCP Snooping database information from the TFTP server or USB drive on reset, if the SNTP is active and synchronized. This means that for the devices that do not re-request a DHCP lease, the MAC and IP address association found in the DHCP Snooping database is restored, and the renew of the IP address or the reboot of the end device is not required.

EAP Fail Open with multi-VLAN

Beginning with Release 5.5, 802.1X EAP Multi-VLAN mode can operate with Fail Open VLAN.

Prior to Release 5.5 when the system lost connectivity to the RADIUS server, the Fail Open VLAN function moved all clients and devices to the Fail Open VLAN. With Release 5.5, the system supports a new mode of operation in conjunction with the Multi-VLAN feature, and multiple concurrent RADIUS VLAN assignments on the port are supported simultaneously.

When you use Release 5.5 or later software to configure a port for EAP Multi-VLAN and then enable EAP Fail Open on that port, if the system loses connectivity to the RADIUS server, all

authenticated clients remain in their respective authenticated VLAN. However, new clients or devices that attempt to connect to the system after connection to the RADIUS server is lost are moved into the Fail Open VLAN until connection to the RADIUS server is reestablished, and re-authentication occurs.

Important:
Avaya recommends that you do not change the multiple VLAN status while Fail Open VLAN is enabled.

Layer 3 Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol (VRRP) is a non-proprietary redundancy protocol described in RFC 3768 designed to increase the availability of default gateway servicing hosts on the same subnet. When Layer 3 enabled VLANs span multiple stacks or separate switches, you can use VRRP to provide default gateway resiliency.

In addition to standard RFC 3768 functions, the switch supports the following extensions:

- Critical IP interface—the ability to specify a certain interface, by IP address, which will trigger the switch to step down from the master role and become a backup router.
- Fast advertisement interval—you can define an advertisement interval that is less the default interval of 1 second. This can be used to improve resiliency where faster VRRP master failure detection is required.
- Ping virtual router—if this feature is enabled, the VRRP router address responds to ICMP echo requests addressed to the virtual IP.

RADIUS EAP or non-EAP requests from different servers

You can now separate RADIUS EAP and non-EAP (NEAP) functions by server. You can configure up to two global RADIUS servers, up to two RADIUS servers, either IPv4 or IPv6, for authentication and accounting of EAP requests, and up to two RADIUS servers, either IPv4 or IPv6, for authentication and accounting of NEAP requests.

Note:
The NEAP RADIUS server is not used for ports in SHSA or MHSA mode.

SLPP Guard

In some customer environments there is a need to provide additional loop protection when used in combination with Avaya's Switch Clustering (SMLT). The Switch Clustering implementations on the VSP9000, ERS8800/8600, and ERS5500 provide a Simple Loop Prevention Protocol (SLPP) packet, which operates to help prevent loops from occurring when Switch Clustering is used.

Simple Loop Prevention Protocol (SLPP) Guard can be used to provide additional loop protection to protect wiring closets from incorrect or faulty connections . When you enable SLPP Guard, this loop prevention mechanism extends into and across multiple wiring closets. If the edge switch configured for SLPP Guard receives an SLPP packet on a port, the feature can immediately disable the port administratively, and generate appropriate log messages and SNMP traps.

Note:

SLPP packets are generated only on switches that are configured with SLPP - for example ERS 5000 Series or ERS 8300. The ERS 4500 switches do not generate SLPP packets locally. When you enable SLPP Guard on an ERS 4500, the switch must be connected to another Avaya switch that supports SLPP and SLPP must be enabled on that switch.

SNMP Trap enhancements

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

STP BPDU filtering ignore-self

You can use the STP BPDU filtering ignore-self parameter to prevent the switch from blocking ports if an IP Phone loops back BPDU packets. When you enable BPDU filtering on the switch port, if you turn off a connected IP Phone, the BPDU packet may be looped back to the switch. The switch can interpret the looping BPDU packet as an attack and block the port administratively. If you have an IP Phone that loops BPDU packets when turned off, Avaya recommends that you enable the ignore-self function.

Unified Authentication

With the introduction of 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. When in stacked mode, the authentication method, username, and local passwords are applied universally across all switches in a stack. If you use the **`cli passwords`** and **`username`** ACLI commands, the unified username, and local passwords are updated on all switches in the stack. The switch updates the obsolete standalone authentication method, username, and local passwords to ensure maximum compatibility, should it become necessary for you to downgrade the switch to a previous software release.

VLACP enhancements

Release 5.5 introduces two additional VLACP message types (DOWN and HOLD) which enable the protocol to better detect and respond to certain one-way communications failures.

In previous releases, if a communication failure occurred on only one link between switches running VLACP, the switch transmitting on the failed link did not detect the failure and continued transmitting VLACP packets. Now the addition of the VLACP Down sub-type enables one switch to provide notification to the other switch of a one-way communication.

Beginning with Release 5.5, you can configure the Ethernet Routing Switch 4500 to receive and process VLACP HOLD messages. A remote device can generate a VLACP HOLD PDU to indicate that the ports are not yet ready to receive traffic. This ensures that all VLACP enabled ports on the remote switch have sufficient time to be ready to receive, and forward ingress traffic before the link is brought into service.

By default, the VLACP HOLD feature is disabled. The feature is enabled by configuring a positive value for VLACP HOLD Time, which matches that of the remote device.

Other changes

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

Enterprise Device Manager enhancements

In Release 5.5 Enterprise Device Manager (EDM) is enhanced with improved data retrieval and request handling for significantly faster GUI response.

In the navigation tree the IP Routing folder is renamed IP and the paths in related procedures have been updated.

The **Switch Summary** tab contents have been enhanced to include basic switch information and stack information.

A toolbar has been added above the EDM navigation tree. The 5 buttons in the toolbar add the following functions:

- **Switch Summary** — you can use the **Switch Summary** toolbar button to open or reopen the switch summary tab.
- **Refresh Status** — in addition to the existing refresh methods you can use the **Refresh Status** toolbar button to refresh the device status.
- **Edit Selected** — in addition to the existing edit methods, and depending on which object you select on the Device Physical View, you can use this toolbar button to open **Edit >**

Chassis, Edit > Unit, or Edit > Ports tabs. If you do not select an object from the Device Physical View and you click the **Edit Select** toolbar button, the **Edit > Chassis** tab opens.

- **Graph Selected** — depending on which object you select on the Device Physical View, you can use this toolbar button to open **Graph > Chassis or Graph > Port** tabs. If you do not make a selection on the Device Physical View, or if you select Unit, the **Graph > Chassis** tab opens.
- **Help Setup Guide** — this button connects you to the help setup guide for embedded EDM and it replaces the link that appeared on the top right of work panes.

For more information, see *Fundamentals Avaya Ethernet Routing Switch 4500 Series* (NN47205-102).

Web server client browser requests

Prior to Release 5.5, when you would run the secure software image with SSL enabled, only HTTPs client browser requests to the Web server were supported. Beginning with Release 5.5, you can use the **`https-only`** command to configure the Web server to respond to both HTTPs and HTTP client browser requests when SSL is enabled.

By default, when you run the secure software image with SSL enabled, the Web server is configured to respond to only HTTPs client browser requests.

If you run the standard software image or if you run the secure software image with SSL disabled, the Web server responds to HTTP client browser requests. In either of these cases, if you attempt to connect to the HTTPs server, the request is automatically redirected to the HTTP server.

You can configure the Web server to respond to both HTTP and HTTPs requests when you run the Secure software image with SSL enabled, by issuing the **`no https-only`** ACLI command. This will then generate a log message to inform you that both server connections are being supported.

Chapter 2: Introduction

This document describes new features, hardware, upgrade alerts, known and resolved issues, and limitations for Avaya Ethernet Routing Switch 4500 Series, Software Release 5.5.

For information on how you can obtain and use the embedded version of Enterprise Device Manager (EDM), see *Avaya Ethernet Routing Switch 4500 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 4500 Series, supported by software release 5.5, 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

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 4500 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 5.5, as well as operational issues not included in the documentation suite.

For a complete list of documentation in the 4500 Series suite, see *Avaya Ethernet Routing Switch 4500 Series Documentation Road Map,* (NN47205-101) .

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

Chapter 3: Important notices

The following sections provide important notices.

Navigation

This section includes the following topics:

Supported software and hardware capabilities

The following table lists supported software and hardware scaling capabilities in Avaya Ethernet Routing Switch 4500 Series Software Release 5.5. The information in this table supersedes information contained in any other document in the suite.

Table 1: Supported software and hardware scaling capabilities

Feature	Maximum number supported
Egress queues	Configurable 1–8
MAC addresses	8000
Stacking bandwidth (full stack of 8 units)	320 Gb/s
QoS precedence	8 per ASIC
QoS rules per ASIC	128 rules per precedence

Feature	Maximum number supported
Maximum number of units in a stack	8
Layer 2	
VLANs	256
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
Spanning Tree Group instances (802.1s)	8
Avaya Spanning Tree Groups	8
DHCP Snooping table entries	1024
Layer 3	
ARP entries (local, static & dynamic)	1792
Local ARP Entries (local IP interfaces)	256
Static ARP entries	256
Dynamic ARP entries	1280
IPv4 route entries (local, static & dynamic)	512
Static routes	32 (configurable 0-256)
Local routes	64 (configurable up to 2-256)
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	16
OSPF Link State Advertisements	10,000
OSPF Virtual Links	4
VRRP Instances	256
Management routes	4
UDP Forwarding entries	128
DHCP relay entries	256
DHCP relay forward paths	512

Feature	Maximum number supported
Miscellaneous	
IGMP multicast groups	512
802.1x (EAP) clients per port, running in MHMA	32
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
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 4500 when various applications are enabled.

Note:
Filters will use the highest available precedence.

Table 2: 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

Feature	Observation	QoS			NonQos	
DHCP Relay	L3 mode	0	0	0	0	0
DHCP Snooping		0	0	0	2	1
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	**Unstrusted**					
	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

Feature	Observation	QoS			NonQos	
OSPF		0	0	0	3	0
RIP		0	0	0	1	0
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 4500 Series, Software Release 5.5 software files. File sizes are approximate.

Table 3: Software Release 5.5 components

Module or file type	Description	File name	File size (bytes)
Standard runtime image software version 5.5.0.002	Standard image for the Avaya Ethernet Routing Switch 4500 Series	4500_550002.img	7,522,228
Secure runtime image software version 5.5.0.003	Secure image for the Avaya Ethernet Routing Switch 4500	4500_550003s.img	7,789,756
Boot/diagnostic software version 5.3.0.3	Switch diagnostic software	4500_5303_diag.bin	1,589,514
Enterprise Device Manager Help Files	Help files required for Avaya Ethernet Routing Switch 4500	ers4500v550_EDM_Help.zip	4,747,512
Enterprise Device Manager plug-in	Avaya Ethernet Routing Swtich 4500 Enterprise Device Manager plug-in for Configuration and Orchestration Manager	ers4500v5.5.0.0.war	6,118,972

Module or file type	Description	File name	File size (bytes)
Software Release 5.5 Management Information Base (MIB) definition files	MIB definition files	Ethernet_Routing_Switch_45xx_MIBs_5.5.0.zip	1,659,870

Supported traps and notifications

For information about SNMP traps generated by the Avaya Ethernet Routing Switch 4500 Series, see Avaya *Ethernet Routing Switch 4500 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 4500 Series Fundamentals,* (NN47205-101).

Upgrading software

To upgrade to the new software release 5.5, Avaya recommends that you upgrade the diagnostic software to the 5.3.0.3 version, and then upgrade the agent version to release 5.5.

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

The following table describes possible image locations:

Table 4: 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

Image	Location
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

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

Important:

A switch that has an agent runtime image prior to release 5.2.0 should not be added to a stack running 5.2.0 or later software. To add a switch with an agent code prior to 5.2.0, you should at a minimum upgrade the agent code, on that unit, to at least 5.2.0 versions before adding the switch to the stack.

When loading software release 5.5 it is mandatory that the switches are loaded with 5.3.0 or later diagnostic software due to the increased size of the 5.5 runtime agent code. The recommended diagnostic version is 5.3.0.3 or later.

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.

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

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

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, or 5.4 to release 5.5 agent image.

Affects of upgrade on 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 5.5, regardless of whether you disabled them prior to the upgrade. When you upgrade from Release 5.4 to Release 5.5 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 nncli
   ```

2. To create an SNMP host using the community you created in the previous step—from the global configuration prompt, enter the following command:

   ```
   snmp-server host 10.100.68.3 port 162 v1 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 nncli
   ```

2. To create an SNMP host using the community you created in the previous step—from the global configuration prompt enter the following command:

   ```
   snmp-server host 10.100.68.3 port 162 v1 CommunityName filter
   TestFilter
   ```

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.

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) server is on the network that is accessible by the switch and that has the desired software version loaded.

OR

- If you change the switch software on a port; 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 24
- Changing switch software in ACLI on page 24
- Changing switch software in EDM on page 26

General software upgrade instructions

Use the following procedure to upgrade the Avaya Ethernet Routing Switch 4500 Series software:

1. Backup the binary configuration file to a TFTP server.
2. Upgrade the boot or diagnostic code, if a new version is available. The system reboots after this step, if you do not specify the **no-reset** option.
3. Upgrade the software image.

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 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 [address <ipv6_address> | <ipv4_address>] {image <image name> | image-if-newer <image name> | diag <image name> | poe_module_image <image name>} [no-reset] [usb] [unit <unit number>]
   ```

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. Depending on network conditions, this process may take up to 8 minutes.

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. Normal switching operations will continue to function..

Job aid—download command parameters

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

Table 5: 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 are mutually exclusive; you can execute only one at a time.	
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 unless software download is to occur using a USB Mass Storage Device.
image *<image name>*	The name of the software image to be downloaded from the TFTP server.
image-if-newer *<image name>*	This parameter is the name of the software image to be downloaded from the TFTP server if it is newer than the currently running image.
diag *<image name>*	The name of the diagnostic image to be downloaded from the TFTP server.
poe_module_image *<image name>*	The name of the Power over Ethernet module image to be downloaded from the TFTP server. This option is available only for 4500 Series switches that support Power Over Ethernet.
no-reset	This parameter forces the switch to not reset after the software download is complete.
usb *[unit <unit number>]*	In the switch, this parameter 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.

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. Depending on network conditions, this process can take up to 8 minutes.

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

Important:
During the download process, the management functionality of the switch is locked. Normal switching operations will continue to function.

Job aid—File System screen fields

The following table describes the File System screen fields.

Table 6: File System screen fields

Field	Description
TftpServerInetAddress	Indicates the IP address of the TFTP server on which the new software images are stored for download.
TftpServerInetAddressType	Indicates the type of TFTP address. • IPv4 • IPv6
BinaryConfigFileName	Indicates the binary configuration file currently associated with the switch. Use this field when you

Field	Description
	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 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.
Action	This group of options represents the actions taken during this file system operation. The options applicable to a software download are • dnldImg: 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. • 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. • dnldConfig: Download a configuration to the switch. • 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. • dnldConfigFromUsb: Download a configuration to switch using the front panel USB port. • dnldImgNoReset: Download a new software image to the switch. This option replaces the

Field	Description
	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. • 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. • upldConfig: Upload a configuration to the switch from a designated location. • 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. • upldImgToUsb: Upload image to USB port • upldConfigToUsb: Upload binary config 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.

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 7: 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> ers4500/ers4500_5.1.0.4.bin
USBascii <*string*>	Specifies the file name of the ASCII configuration file to load from the USB device. Example: customer1.cfg
USBagent <*string*> NEXTIP, NEXTMask, and NEXTGateway	Specifies the file name of the agent image to load from the USB device and specifies IP addresses for the next boot. Example: ers4500/ers4500_5.2.0.0.img

The ip.cfg file loads information from the ASCII configuration file in order of precedence.

For example, if you have an ip.cfg file with the following commands:

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

The stack IP becomes 181.30.30.113 no matter what IP address is in the config.txt file. If you have an ip.cfg file with the following commands:

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

The stack IP will be the IP address if it is defined in the config.txt file.

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.

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 Avaya Ethernet Routing Switch 4500 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 4500 banner page appears while the switch retrieves the ip.cfg file.

Important:

While the system retrieves the ip.cfg file from the USB memory device, the Avaya banner page appears. If you use the serial console while the system restarts, you will see the Avaya banner page during the restart. Do not attempt to access the switch for at least three minutes.

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 opens the first page of menu.
- 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 and SFP transceiver compatibility

The following table lists the XFP and SFP transceiver compatibility.

Table 8: XFP and SFP transceiver compatibility

Supported SFPs and XFPs	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
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

Supported SFPs and XFPs	Description	Minimum software version	Part number
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
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	1550nm LC connector, up to 40km	5.4.0	AA1419057-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	AA1419063-E6

Supported SFPs and XFPs	Description	Minimum software version	Part number
1000BaseCWDM DDI SFP	1530nm LC connector, up to 70km	5.4	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
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, 120km.	5.4.0	AA1419071-E6
100BASE-FX SFP	1310 nm LC connector	5.0.0	AA1419074-E6
T1 SFP	1.544 Mbit/s 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 SFP 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
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

For more information, see *Avaya Ethernet Routing Switch 4500 Series Installation,* (NN47205-300).

Supported standards, RFCs and MIBs

The following sections list the standards, RFCs and MIBs supported in Release 5.5.

Standards

The following IEEE Standards contain information pertinent to the Avaya Ethernet Routing Switch 4500 Series:

- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.3 (Ethernet)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1s (Multiple Spanning Trees)
- IEEE 802.1w (Rapid Reconfiguration of Spanning Tree)
- IEEE 802.1X (EAPOL)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.1v (VLAN Classification by Protocol and Port)
- IEEE 802.3z (Gigabit Ethernet)
- IEEE 802.3ab (Gigabit Ethernet over Copper)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3af (Power over Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (Gigabit Ethernet over Fiber-Optic)

RFCs and MIBs

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

- RFC 791 (IP)
- RFC 894 (IP over Ethernet)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 826 (ARP)
- RFC 768 (UDP)
- RFC 854 (Telnet)
- RFC 951 (BootP)
- RFC 1058 (RIP v1)
- RFC 1213 (MIB-II)
- RFC 1350 (TFTP)
- RFC 1493 (Bridge MIB)
- RFC 2863 (Interfaces Group MIB)
- RFC 2665 (Ethernet MIB)
- RFC 2737 (Entity MIBv2)
- RFC 2819 (RMON MIB)
- RFC 1757 (RMON)
- RFC 1271 (RMON)
- RFC 1157 (SNMP)
- RFC 1112 (IGMPv1)
- RFC 2236 (IGMPv2)
- RFC 1945 (HTTP v1.0)
- RFC 2865 (RADIUS)
- RFC 2674 (Q-BRIDGE-MIB)
- RFC 3410 (SNMPv3)
- RFC 3411 (SNMP Frameworks)
- RFC 3413 (SNMPv3 Applications)

- RFC 3414 (SNMPv3 USM)
- RFC 3415 (SNMPv3 VACM)
- RFC 3412 (SNMP Message Processing)
- RFC 3576 Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
- RFC 4673 RADIUS Dynamic Authorization Server MIB
- RFC 2131 BootP/DHCP Relay Agent
- RFC 1583 (OSPF v2)
- RFC 1850 (OSPF v2 MIB)
- RFC 2328 (OSPF v2)
- RFC 2453 (RIP v2)
- RFC 2474 (Diffserv)
- RFC 2475 (Diffserv)
- RFC 2866 (RADIUS Accounting)
- RFC 3046 (DHCP Relay Agent Information Option)
- RFC 3768 (Virtual Router Redundancy Protocol)
- RFC 3993 (DHCP Subscriber-ID suboption)
- RFC 3917 (IP Flow Information Export [IPFix])
- RFC 3954 (Netflow Services Export v9)

IPv6 specific RFCs

The following table lists IPv6 specific RFCs.

Table 9: Supported IPv6 specific RFCs

Standard	Description	Compliance
RFC 2460	Internet Protocol v6 (IPv6) Specification	Supported
RFC 2461	Neighbor Discovery for IPv6	Supported
RFC 2462	IPv6 Stateless Address Auto-configuration	Auto-configuration of link local addresses only
RFC 4443	Internet Control Message Protocol (ICMPv6)	Support earlier version of RFC (2463)

Standard	Description	Compliance
RFC 4301	Security Architecture for the Internet Protocol	Not supported
RFC 4291	IPv6 Addressing Architecture	Support earlier version of RFC (3513)
RFC 4007	Scoped Address Architecture	Supported
RFC 4193	Unique Local IPv6 Unicast Addresses	Not supported
RFC 4293	Management Information Base for IP	Mostly supported
RFC 4022	Management Information Base for TCP	Mostly supported
RFC 4113	Management Information Base for UDP	Mostly supported
RFC 1981	Path MTU Discovery for IPv6	Supported
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks	Supported
RFC 4213	Transition Mechanisms for IPv6 Hosts and Routers	Supports dual stack. No support for tunneling yet.
RFC 3162	RADIUS and IPv6	Supported
RFC 1886	DNS Extensions to support IPv6	Supported

Chapter 4: Resolved issues

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

Resolved issues for Release 5.5

The following table lists the issues resolved for release 5.5.

Reference number	Description
wi00484230	**IPv6**: An inconsistency between how the default gateway for IPv4 or IPv6 is deleted or defaulted is now addressed.
wi00484338	**Energy Saver, SNMP Traps**: SNMP Traps as well as log messages are now generated for AES events.
wi00484371	**EAP, RFC3756**: EAP clients which use RFC3576 CoA are now properly handled after a reset of the stack.
wi00491241	**ADAC, MLT/DMLT/LAG**: If MLT/DMLT or LAG ports are configured for an ADAC uplink, they are now correctly displayed when issuing the show adac command.
wi00491266	**TACACS+**: You can now delete or default individual TACACS+ server configurations (previously you had do delete or default both servers if configured).
wi00491353	**Fan Failure Log Message**: An improved log message is now generated indicating if a fan should fail or become degraded, including the fan number.
wi00491479, wi00497658	**DHCP Client**: If the switch or stack has obtained the management IP address via DHCP and is rebooted, then a DHCP release message is now sent So that the IP Lease is correctly released from the DHCP server.
wi00491574	**DHCP option 82, ACG**: ASCII configuration output for DHCP Option 82 now produces output using port number ranges, which reduces the size of the generated output.
wi00491655	**IP.CFG**: The switch will now continue to process ip.cfg until the end of the file, even if the file contains some errors.
wi00491664	**IPFiX**: IPFiX now provides TCP flag information in the templates which are exported to IPFiX collectors.

Reference number	Description
wi00554878	**TDR**: When attempting to perform TDR function on fibre ports on the 4526FX, the switch now correctly indicates that TDR can only be performed on copper ports.
wi00554909	**NEAP, RADIUS Accounting**: RADIUS Accounting & Interim Updates are now supported for Non-EAP (NEAP) devices.
wi00555059, wi00555262	**TACACS+**: The switch now correctly sets the same user-is for both the authentication and authorization phases. This allows the TACACS+ server to correctly track the user and appropriate commands issued.
wi00555099	**TACACS+**: The user is now authenticated at the correct privilege level as defined by the TACACS+ server configuration.
wi00675085	**LACP**: A link with LACP configured now correctly remain inactive when partner sync flag is not set. This now correctly prevents certain blackhole traffic scenarios which could have eventuated.
wi00691368	**DHCP Snooping, IP Source Guard (IPSG), Windows PXE**: The IP Address of a windows PXE system is now correctly cleared from the DHCP Snooping and IPSG bindings when the client is disconnected or shutdown.
wi00691675, wi00691676, wi00554900	**EAP, STP**: The switch now send the first authentication request to the client when the port enters forwarding state (if STP is enabled), rather than when the link first becomes active. This reduces the EAP failures which may have been seen in some customer scenarios when the client first connects to the port.
wi00692262	**Static Route**: An IP Static Route now correctly remains active in certain scenarios where the physical interface is up and switch is able to reach the remote IP interface.
wi00703941	**RIP, Cisco Interoperability**: The ERS4500 now correctly accepts RIP updates from some Cisco routers which may send RIP updates with a destination of 255.255.255.255 (all ones) rather than using the subnet broadcast address.
wi00727220	**Port Mirroring**: Traffic generated by the switch CPU (for example ping message) is not correctly mirrored to the mirror port.
wi00491359	**SNMP Traps**: When you use the CLI commands **`show snmp-server host`** and **`show snmp-server notify-filter`** there is now a correlation between which filter is applied to which host.
wi00555056	**ADAC, MLT, ACG**: If you configure ADAC uplink or call server ports on a switch to be a member of an MLT/DMLT or LAG, then the ASCII configuration file generated by the switch no longer contains an error in the "adac uplink-port" or "adac call-server-port" definitions.

Reference number	Description
wi00491700	**Port Mirroring**: If you set port mirroring to AsrcBdstOrBsrcAdst mode, the switch mirrors Layer 2 broadcast traffic with a MAC source address that equals Asrc to the monitor port.
wi00491583	**ADAC, LLDP, EAP**: If an IP Phone has already been detected by ADAC and LLDP and then you subsequently configure NEAP IP Phone capability, the port now will authenticate the IP Phone via its DHCP signature.
wi00854383	**802.1AB/ LLDP-MED**: The switch will now correctly limits the characters which can be entered into ecs-elin for lldp med location-identification to only printable characters.
wi00846039	**802.1X/NEAP, Microsoft Network Policy Server**: When Non-EAP (NEAP) authentication is performed to a Microsoft Network Policy Server the NAS-Port-Type is now correctly set to “Ethernet” so that authentication can be properly be performed.
wi00555100, wi00555272	**ACG/Rate-Limiting**: A missing exit statement at the end of the rate limiting section is now correctly displayed in the ASCII configuration generated by **`show running-config`**.
wi00858158	**ADAC/Avaya 9600 IP Phones**: ADAC automatic configuration is now correctly applied to all Avaya 9600 IP Phones when connected to switch ports provisioned for ADAC.
wi00704055	**ADAC/DMLT**: If ADAC is configured to use DMLT as an uplink port and if a unit in the stack containing one of the DMLT links is powered down, ADAC will now continue to use the remaining DMLT links correctly.
wi00856195	**ADAC/DMLT**: When ADAC is configured with DMLT as uplink ports, traffic is now correctly prioritized on all links in the trunk.
wi00864240	**ADAC**: When ADAC is configured with uplink ports which are not on the base unit, network policies are now correctly set on all uplink ports.
wi00836972	**CLI / Scripts**: When running multiple simultaneous scripts which poll the switch to retrieve ASCII and binary configuration in combination with SNMP polling, the switch management interface will no longer lock-up waiting for CLIAudit event. It is recommended if customers do regularly perform multiple simultaneous scripts and SNMP polling that autosave is disabled.
wi00835594	**DHCP Relay**: When the switch is performing DHCP relay, the DHCP Unicast acknowledge (option 85) is no longer incorrectly changed to a multicast acknowledge.
wi00839101	**IGMP**: When an IGMP Querier exists on the network, the switch no longer incorrectly generates it own IGMP general query messages.
wi00858143	**MAC Security**: If more than the maximum of 448 MAC addresses are learnt with MAC Security auto learn enabled, then these addresses are

Reference number	Description
	cleared from the MAC Security table, the switch will now correct re-learn up to the maximum number of 448 MAC Security Addresses.
wi00847984	**MAC Security**: Inconsistency when MAC Security learning is set to automatic between information displayed MAC Address Table and MAC Security Addresses is rectified.
wi00831512	**MAC Security**: When a port down event occurs, Static or Sticky MAC addresses are no longer incorrectly removed from the MAC security list.
wi00848022	**MAC Security**: When MAC Security learning is set to automatic, entries can now be correctly cleared from the MAC Security and MAC Address tables when either the port or MAC Security is disabled.
wi00817070, wi00554903	**SNTP, Autosave**: Settings for SNTP are now correctly saved when autosave is disabled.
wi00491097	**EDM**: Can now support the selection of multiple ports to create graphs. Note: that when using Firefox, you can only select one item when using the shift key to attempt to select multiple cells to graph.
wi00483756	**Energy Saver**: Energy savings displayed for 4526FX is now correctly reported after AES is activated.
wi00491677	**Energy Saver, SNTP**: If energy saver is enabled and a local schedule is defined, a guard-rail now prevents you from disabling SNTP.
wi00484157	**EAP, Multi-VLAN, ADAC**: When operating in Multi-VLAN EAP/NEAP mode and ADAC is operating in untagged frames basic mode, the port is correctly moved from the Guest VLAN/PVID.
wi00484159	**EAP**: When operating in Multi-VLAN EAP/NEAP mode and ADAC is operating in tagged frames mode, the port is correctly moved from the Guest VLAN/PVID.
wi00863709	**NEAP, Multi-VLAN**: When NEAP authentication is configured with multi-VLAN enabled, if the VLAN priority is changed on server, the change is now correctly displayed with the **`show eapol mulihost non-eap-mac-status`** command.
wi00483951	**ADAC, MLT**: When an ADAC uplink port is defined using a MLT, DMLT, or LAC, now all ports of the MLT, DMLT, or LAC will be displayed.
wi00484340	**ADAC, EAP, Guest VLAN**: If you configure both Guest VLAN (GVLAN) and ADAC on a port and the system receives an EAP logoff message, the port is now correctly moved correctly back into the GVLAN.
wi00555056, wi00555254	**ADAC, MLT, ACG**: If you configure ADAC uplink or call-server ports on a switch to be a member of a MLT/DMLT or LAG, then the ASCII configuration file generated by the switch no longer contain an error in the "adac uplink-port" or "adac call-server-port" definitions.

Reference number	Description
wi00555072	**VLACP**: VLACP now supports the “Down” subtype which enabled VLACP to better detect certain types of uni-drectional faults which would have previously left the link as operational.
wi00554906	**AUR**: AUR now supports the ability to remove a units MAC address from the AUR cache. This can be used for demonstration or troubleshooting purposes by allowing a unit with it’s MAC Address removed to act as if it were a replacement unit in a stack.
wi00868704, wi00869601, wi00845260	**HTTP/HTTPs**: Change in operation of HTTP and HTTPs on secure software image now allows HTTP and HTTPs to be separately configured.
wi00483986	**EDM**: EDM now supports the ability to indentify unit numbers in stack.
wi00831097	**EDM, PoE**: The port PoE status is now correctly displayed in the EDM device physical view.
wi00484234	**NEAP, DHCP Signature**: The VLAN ID and priority of the DHCP signature authenticated client is now correctly displayed.
wi00484146	**IPFiX**: When displaying the top-50 entries from the IPFiX table when there is a larger number of records, there is now longer a large delay after issuing the ACLI command.
wi00490991	**IPFiX**: Collectors are now correctly displayed per stack, rather than per unit.
wi00685932	**DHCP Snooping**: The output will remain consistent if you repeatedly issue the show ip dhcp-snooping binding command.
wi00692577	**Packet Counters**: OutDiscards packets are now correctly counted rather than being counted as filtered packets.
wi00716524	**ADAC, MLT**: ADAC MLT uplink ports are now correctly removed from the Voice VLAN when the MLT is deleted.
wi00733367	**Static ARP**: Static ARP entries are now correctly maintained if the switch looses power or you issue a clear ARP command.
wi00851594	**MAC Security**: The s5EtrNewSbsMacAccessViolation trap is now correctly generated when Sticky MAC security is enabled and an intruder MAC occurs.

Chapter 5: Known issues and limitations

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

Known issues and limitations for Release 5.5

The following table lists known issues and limitations for Avaya Ethernet Routing Switch 4500 Series Software Release 5.5.

Reference number	Description
wi00885951	**Autotopology, SONMP**: If the Ethernet Routing Switch 4500 is connected to ERS 8800 with 8895CPU or 8810/8806,8803R chassis; then the ERS 4500 will report these as unknown devices in the SONMP autotopology table.
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 re-acquire 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.
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.
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.
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

Reference number	Description
	manual 802.1AB-MED network policy will 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.
wi00861372	**802.1AB Integration / Call Server TLV**: You can configure up to 8 Call Server IP Addresses on the switch for maximum resiliency. When 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.
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 fileserver, ensure that the File Server TLV is appropriately configured.
wi00834767	The maximum number of streams monitored by IPFIX is 100.000.
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 because this is an obsolete command. See Unified password authentication for more details about new command syntax..

Reference number	Description
wi00841212	**EDM, TACACS+**: EDM does not have the option to set authentication type to TACACS+. Use ACLI if this type of authentication is desired for the switch.
wi00841955	**LLDP 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.
wi00846698	**EDM**: EDM multiport select does not work on interfaces with SFPs/XFPs inserted. Please use per port configuration for interfaces with optics installed.
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 initial value instead of remain 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.
wi00855310	**EAP, NEAP IP Phone, DHCP Signature**: EAP authentication by DHCP signature currently only works for legacy Nortel IP Phones and not for Avaya IP Phones. **Workaround**: You can use other means of client authentication with Avaya IP Phones.
wi00858022	**LLDP 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.
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).
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 mis-match 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.
wi00862047	**802.1AB Integration / Phone IP TLV**: If the Avaya IP Phone receives it’s IP Address from a DHCP sever 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.
wi00862054	**802.1AB VLAN Name TLV**: When the command **`lldp tx-tlv dot1 port-protocol-VLAN-id VLAN-name`** is issued on an

Reference number	Description
	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.
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.
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".
wi00863190	**NEAP, Interim Updates**: When Interim updates are enabled for non-EAP (NEAP) clients, then in some cases the switch will send a duplicate interim-update with all values set to null.
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.
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.
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 to turn off interim updates also, if it is not desired receiving them.
wi00865086	**802.1AB MED Network Policy, DHCP Option242**: When DHCP Option 242 is used to specify the Voice VLAN (L2QVLAN) for an Avaya IP Phone it is necessary to remove the 802.1AB/LLDP MED policy VLAN from the switch, so that the IP Phone will correctly use the Voice VLAN specified by DHCP option 242. Workaround: For the Avaya IP Phone to remain configured with the IP address from voice VLAN, delete the default LLDP MED network policy using the interface command **`no lldp med-network-policies`**.
wi00868382	**802.1AB / LLDP Default Parameters, ADAC**: In the current release, with the introduction of 802.1AB default parameters a default LLDP MED policy is configured from the start on all ports. The default values for that policy is 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 never be

Reference number	Description
	installed, resulting in the IP phone not receiving the VLAN configuration, in case ADAC tagged frames is used. The same behavior applies to ADAC uplink/call server ports. This happens because the default MED policy is static and overrides the dynamic one that should be 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.
wi00872224	**PoE Traps**: The pethPsePortOnOffNotification trap can be configured per interface on a non-PoE switch if a non-PoE switch is the base unit. This has no affect on the functionality as non-poe ports will never generate traps related to PoE.
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>`**.
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 (eg 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>`**.
wi00880382	**DHCP Snooping External Save**: If a stack is transitioning to standalone mode, then the log message generated by DHCP External Save may contain incorrect information for the USB unit number.
wi00490844	**IP Source Guard (IPSG), Traps**: If the maximum IP entries has been learnt on a MLT/LACP enabled port, then is that trunk is disabled additional log messages are generated.
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.

Reference number	Description
wi00841065	**802.1AB MED Network Policy**: When upgrading to 5.5 software and the previous configuration contained no network policies, the new default network policies for 5.5 release will be applied.
wi00863027	**802.1AB Default Values**: When you upgrade to 5.5 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).
wi00876311	**EDM**: 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.

Known issues and limitations for releases prior to Release 5.5

The following section lists known issues and limitations in Avaya Ethernet Routing Switch 4500 Series software releases prior to Release 5.5.

Table 10: Known issues and limitations

Reference number	Description
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.
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 4500 switch. You can ignore this auto topology change message where there is a direct connection from the Avaya ERS 4500 to a BayStack 450 switch.
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

Reference number	Description
	ASCII configuration from EDM to a switch or stack that has a basic configuration. Alternatively, a currently-configured switch/stack can be reconfigured using an ASCII configuration via CLI (console, telnet, SSH) since the system ignores warning and error messages and configuration continues until the last ASCII file line executes.
wi00489936	**Jumbo Frames**: As the Avaya Ethernet Routing Switch 4500 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.
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.
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 through they are actually in the Green VLAN.**Workaround**: Execute the CLI commands **`shutdown`**, then **`no shutdown`** on the corresponding ports.
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).
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.
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 precedences 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 configuration file may be reloaded incorrectly. If the QoS information in the binary configuration file is reloaded incorrectly, some of the QoS precedences may not be configured correctly.
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

Reference number	Description
	displayed when you use the CLI command **`show IPv6 TCP connection`**. This behavior is considered normal. **Workaround**: If simultaneous Web page refresh commands are issued, then a **`show ipv6 tcp connection`** command displays the active TCP connections for the Web session.
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.
wi00483629	**NSNA**: If you add a new classifier to the NSNA yellow QoS set (exceeding the resources), the yellow filters may not be applied.
wi00483626	**MLT/DMLT**: It may be possible to change the VLAN membership of administratively disabled MLT/DMLT ports. 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. If you want to change the VLAN membership for a MLT/DMLT group, you must: • Disable all ports which are members of that group or disable the MLT/DMLT. • Make the necessary VLAN changes to all group members. • Re-enable the port or MLT/DMLT.
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.
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.
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.
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

Reference number	Description
	either the one manually configured for that port or the one received for the previous authenticated client.
wi00483752	**Port Mirroring**: The port mirroring modes asrc and adst cannot mirror packets generated by the CPU such as: LACPDUs, LLDPDUs, BPDUs, and SONMP.**Workaround**: CPU-generated packets can be mirrored with port-mirroring mode XTX.
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.
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.
wi00483813	**EDM, Energy Saver**: EDM does not display the PoE Savings and PoE Priority in the energy saver ports tab. **Workaround**: Use the CLI command **`show energy-saver interface`** to display information about energy saver and PoE savings port status.
wi00483820	**EDM, TACACS+**: You cannot use EDM to enable TACACS+ because, when you enable TACACS+, the system disables Web access to the switch. If you used EDM to enable TACACS+ you would lose EDM access for any subsequent operations.
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 reenabled by VLACP .`
wi00491450	**Port Mirroring**: If you use port 1 as a mirror port in XrxYtx or XrxYtxOrYrxXtx 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.
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

Reference number	Description
	to best assure that the minimum rates for the rest of the queues are achieved. Note: If you have ERS 4500 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.
wi00491375	**EAP Packet-Mode**: The default EAP packet mode on the switch is set to multicast. When the EAP packet mode is set to multicast, the switch continues to send EAP requests at defined intervals (default is 30 seconds) until the maximum number of EAP clients configured for the port is reached. This behaviour is required for some EAP devices that need to receive a Request Identity in order to start EAP. Workaround: If your EAP client devices do not require Request Identity in order to start EAP, you can set the EAP packet mode to Unicast.
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.
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.
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 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.
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 behavor 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 re-create the SNMPv3 users after loading the ASCII configuration.
Q02107731	**OSPF, Scaling**: When you run OSPF with a high number of adjacencies (for example 64 OSPF neighbors) it is recommended that the total number of Link State Advertisement (LSA) entries in the OSPF Link State Database (LSDB) should not exceed 10,000.

Reference number	Description
wi00491271, wi00484313	**BX SFPs**: When you connect two BX SFPs (Part Code AA1419069-E6 and AA1419070-E6) between Gigabit ERS 4500 switches, in some cases the link may not be established. This has been found to occur only if the vendor of the BX SFP is Luminet (as identified by the vendor serial number starting with LUMNT) and the SFP is revision A. Workaround: To correctly establish the link, replace one of the BX SFPs with a later revision SFP.
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
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 indicates 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 assocaition.
wi00491537	**EDM**: To copy and paste text between text boxes in EDM you can use the keyboard shortcuts `Ctrl+C` to copy text and `Ctrl+V` to paste text.
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 re-acquire 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 re-learns 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.
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 neighbour 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

Reference number	Description
	ports for OSPF adjacencies or RIP route connections, energy saver will not cause a link transition.
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. Alternative: you can globally disable EAP, configure GVLAN, then re-enable EAP globally.
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.
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.
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.
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.

IPv6 limitations

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

Table 11: 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 6: 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.