



# **Release Notes — Software Release 4.4 Avaya Ethernet Routing Switch 2500 Series**

4.4  
NN47215-400, 05.02  
August 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/](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

<b>Chapter 1: Introduction</b>	<b>5</b>
<b>Chapter 2: New in this release</b>	<b>7</b>
802.1AB (LLDP) Customization	7
802.1AB (LLDP) integration	7
802.1X NEAP and Guest VLAN on same port	7
802.1X NEAP Last Assigned RADIUS VLAN	7
802.1X NEAP re-authentication	8
802.1X NEAP with Fail Open VLAN	8
ADAC enhancements	8
Asset ID configuration	8
DHCP option 82 support	9
DHCP Server	9
Diagnostics Auto Unit Replacement (DAUR)	9
Dual Syslog Server Support	9
IGMPv3 proxy	9
IGMPv3 Snooping	10
IPv6 protocol-based VLANs	10
Layer 3 Non-Local Static Routes (IP NLSR)	10
MLT enable or disable whole trunk	10
RADIUS EAP or non-EAP requests from different servers	11
RADIUS Server Reachability	11
Secure File Transfer Protocol (SFTP over SSH)	11
SSH enhancement to support RSA	11
Show environmental	12
Show Software Status	12
Sticky MAC address	12
Basic management TLV set	12
Other changes	13
<b>Chapter 3: Important notices and new features</b>	<b>15</b>
File names for this release	15
Secure software image	16
Software upgrade instructions	16
Supported software and hardware capabilities	16
Getting EDM online help files for embedded EDM	18
Downloading help files	18
Configuring the path to the help files	20
Configuring the path to the help files using EDM	20
SFP transceiver compatibility	21
Important note on use of the two rear 1000Base-T (RJ-45) ports (all models)	23
Supported standards, RFCs and MIBs	24
Standards	24
RFCs and MIBs	25
<b>Chapter 4: Resolved issues</b>	<b>29</b>
<b>Chapter 5: Known issues and limitations</b>	<b>31</b>

Known issues.....	31
Known limitations.....	38

# Chapter 1: Introduction

This document describes new features, hardware, upgrade alerts, known and resolved issues, and limitations for Avaya Ethernet Routing Switch 2500 Series, software release 4.4.

The Avaya Ethernet Routing Switch 2500 Series, supported by software release 4.4, includes the following switch models:

- Avaya Ethernet Routing Switch 2526T
- Avaya Ethernet Routing Switch 2550T
- Avaya Ethernet Routing Switch 2526T-PWR
- Avaya Ethernet Routing Switch 2550T-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 2500 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 4.4, as well as operational issues not included in the documentation suite.

For a complete list of documentation in the 2500 Series suite, see *Avaya Ethernet Routing Switch 2500 Series Documentation Road Map* (NN47215-103).

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



# Chapter 2: New in this release

The following sections describe what's new in Avaya Ethernet Routing Switch 2500 Series release 4.4.

---

## 802.1AB (LLDP) Customization

802.1AB customization supports a set of enhancements to LLDP with a wider range of industry standard system Type, Length, and Value (TLV) parameters and timer configurations.

---

## 802.1AB (LLDP) integration

802.1AB integration supports a set of enhancements to 802.1AB (LLDP) Type, Length, and Value (TLV) parameters to support Avaya IP Telephones.

---

## 802.1X NEAP and Guest VLAN on same port

With this enhancement you can now configure the 802.1X, Non-EAP, and Guest VLAN functions on the same port simultaneously for a more universal port configuration. You do not have to configure a port to support Guest VLANs or Non-EAP or 802.1X; one port can support all three functions.

---

## 802.1X NEAP Last Assigned RADIUS VLAN

The 802.1X NEAP Last Assigned RADIUS VLAN feature allows an EAP or non-EAP client to use the most recent RADIUS assigned VLAN. The Last Assigned RADIUS VLAN determines the VLAN membership and PVID values for the port.

---

## 802.1X NEAP re-authentication

You can use NEAP (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.

---

## 802.1X NEAP with Fail Open VLAN

802.1X NEAP with fail open VLAN provides network connectivity when the switch cannot connect to the RADIUS server. If connectivity to the RADIUS servers is lost, all authenticated devices move into the configured fail open VLAN.

---

## ADAC enhancements

Auto-Detect Auto-Configuration (ADAC) enhancements provide increased flexibility in deployments that use ADAC as follows:

- Expanded support for up to eight ADAC uplinks and eight Call Server links (individual ports or any combination of MLT, DMLT, or LAG) for each switch or stack.
- Ability to change the non-ADAC VLANs on a port without disabling ADAC.

---

## Asset ID configuration

You can configure the Asset ID with CLI commands or EDM. An Asset ID provides inventory information for the switch, stack, or each unit within a stack.

---

## DHCP option 82 support

DHCP option 82 is an extension of Dynamic Host Configuration Protocol (RFC3046 and RFC3993) that enables the switch to send information about DHCP clients to the authenticating DHCP server to assist in tracking end device locations.

---

## DHCP Server

If you require local provision of TCP/IP addresses and have no separate DHCP Server or other device available to provide the service to local hosts, DHCP Server is included on the switch. You can use the DHCP Server feature to provide and manage client IPv4 addresses in your network and eliminate manual TCP/IP configuration. DHCP Server is disabled by default.

---

## Diagnostics Auto Unit Replacement (DAUR)

The switch uses Diagnostic Auto Unit Replacement (DAUR) to update the diagnostic image on a non-base unit with the diagnostic image saved in the base unit of a stack, if the images differ. When you enable or disable Agent Auto Unit Replacement (AAUR), you automatically enable or disable DAUR in conjunction with AUR. The default setting for AAUR and DAUR is enabled.

---

## Dual Syslog Server Support

You can use the Dual Syslog Server support feature to configure a second syslog server to run in tandem with the first. If you configure two Syslog server IP addresses, the switch sends Syslog messages to both servers simultaneously to ensure that Syslog messages are recorded, even if one of the servers becomes unavailable.

---

## IGMPv3 proxy

With IGMPv3 proxy enabled, if the switch receives multiple reports for the same multicast group, it does not transmit each report to the upstream multicast router. Instead, the switch forwards the first report to the querier and suppresses the rest.

If new information emerges, for example if the switch adds another multicast group or receives a query since the last report was transmitted upstream, then the switch forwards a new report to the multicast router ports.

---

## IGMPv3 Snooping

In IGMPv3 snooping mode, the switch recognizes IGMPv3 reports and queries and can:

- recognize whether a source list is populated or blank
- identify the specific sources to filter for every multicast group a client joins to
- understand and process all IGMPv3 query types, INCLUDE and EXCLUDE IGMPv3 report types

The following are supported:

source filtering based on ALLOW and BLOCK, IGMPv3 report types

---

## IPv6 protocol-based VLANs

IPv6 recognition through the configuration of protocol-based VLANs for segmenting IPv6 traffic is supported.

---

## Layer 3 Non-Local Static Routes (IP NLSR)

You can use IP NLSR when the next-hop IP address is not directly reachable from the switch or when there are multiple paths to a network but the number of static routes can be reduced by using only one route with a remote gateway.

---

## MLT enable or disable whole trunk

Use the Multi-Link Trunk (MLT) enable or disable whole trunk feature to enable or disable trunk loop prevention for MLT or Distributed MLT (DMLT). The feature is disabled by default. If you enable the feature, the state of the port changes to reflect the state of the MLT or DMLT bundle irrespective of the previous status. If you disable the MLT or DMLT then all links that are part of the MLT group are disabled, with the exception of the Destination Lookup Failure (DLF) link. For network configuration, Avaya recommends you to enable the MLT whole trunk feature.

---

## RADIUS EAP or non-EAP requests from different servers

You can now separate EAP and non-EAP functions by server. You can configure up to two RADIUS servers, either IPv4 or IPv6, for authentication and accounting of EAP requests and up to two servers, either IPv4 or IPv6, for authentication and accounting of non-EAP requests. NOTE: the non-EAP RADIUS server is not used for ports in SHSA or MHSA mode since neither mode supports non-EAP.

---

## RADIUS Server Reachability

You can use RADIUS server reachability to configure the switch to use ICMP packets or dummy RADIUS requests to determine the reachability of the RADIUS server. The switch regularly performs the reachability test to determine if the switch should fail over to the secondary RADIUS server or to activate the fail open VLAN, if that feature is configured on the switch. If you implement internal firewalls which limit the flow of ICMP reachability messages from the switch to the RADIUS server, you can configure the switch to use dummy RADIUS requests. If the switch is configured to use dummy RADIUS requests, the switch generates a regular dummy RADIUS request with the username 'avaya'. It is recommended that you set up a dummy account with the user name avaya on the RADIUS server to avoid the generation of error messages indicating invalid user logins, if RADIUS server reachability is enabled. By default, the switch uses ICMP packets to determine the reachability of the RADIUS server.

---

## Secure File Transfer Protocol (SFTP over SSH)

To provide secure file transfer functions, release 4.4 and up includes support for Secure FTP over a Secure Shell (SSH) session to the switch. Secure FTP on the ERS2500 series only allows transfer of the binary configuration file.

---

## SSH enhancement to support RSA

When you select the RSA certificate option for a Secure Shell connection to the switch for a client PC, RSA public-private key encryption using a digital certificate with SSH login, is supported as a background option.

---

## Show environmental

You can use this feature to display environmental information about the operation of the switch or units within a stack. The information includes power supply status, fan status, and switch system temperature.

---

## Show Software Status

The **show boot** CLI command or the Boot Image EDM tab can display the currently loaded and operational software status for both agent and diagnostic images.

---

## Sticky MAC address

Sticky MAC address provides a high level of control and simpler configuration and operation for MAC address security. Sticky MAC address secures the MAC address to a specified port so that if the address moves to another port, the system raises an intrusion event. When you use Sticky MAC address, the switch performs initial auto-learning of MAC addresses and can store the automatically-learned addresses across switch reboots.

---

## Basic management TLV set

The basic management TLV set contains the following TLVs:

- **Port Description TLV**
- **System Name TLV**
- **System Description TLV**
- **System Capabilities TLV** (indicates both the system supported capabilities and enabled capabilities, such as end station, bridge, or router)
- **Management Address TLV**

Beginning with Release 4.4 the switch supports IPv4 and IPv6 management addresses and the transmission of all TLVs from the basic management TLV set is enabled by default.

---

## Other changes

### Enterprise Device Manager (EDM) enhancements

In Release 4.4 EDM has been enhanced with improved data retrieval and request handling for 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 view 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

New in this release

# Chapter 3: Important notices and new features

This section contains a brief synopsis of the new features in release 4.4 and any important notices.

---

## File names for this release

The following table describes the Avaya Ethernet Routing Switch 2500 Series software release 4.4 software files.

Release 4.4 EDM help files are available as follows:

- A downloadable zip file, `Ethernet_Routing_Switch_25xx_EDM_Help_4.x.x.zip`
- On the CD-ROM inside the ERS 2500 v4.x.x Base Software License Kit folder contained in the switch shipping box

**Table 1: Software release 4.4 components**

File description	File name
Standard (non-SSH) runtime image software version 4.x.x	2500_4.4.0.010.img
Secure (SSH) runtime image software version 4.x.x	2500_4.4.0.011s.img
Boot/Diagnostic software version for 1.0.0.15	2500_10015_diag.bin
Software Release 4.x Management Information Base (MIB) definition files	Ethernet_Routing_Switch_25xx_MIBs_4.4.0.zip
EDM Help files zip	Embedded: Ethernet_Routing_Switch_25xx_EDM_Help_4.4 .0.zip COM plug in: Ethernet_Routing_Switch_25xx_EDM_Plugin_4 .4.0.zipp

---

## Secure software image

The Ethernet Routing Switch Software can be installed using a secure image that provides the following features:

- Secure Shell (SSH) connections
- SHA-based user authentication and DES-based privacy encryption

These features are not available with the standard software image.

---

## Software upgrade instructions

To upgrade to Release 4.4 switch software you must use the procedure in this section or the upgrade will fail. The size of the Release 4.4 software image is greater than 6 MB and the 1.0.0.15 diagnostics code in the procedure can boot images exceeding 6 MB, but previous diagnostic code versions cannot.



### **Warning:**

You must use the following procedure to upgrade the switch software to Release 4.4 or the upgrade will fail.

If you are using a release prior to Release 4.3, you must first upgrade to Release 4.2.4 before proceeding with the upgrade to Release 4.4.

1. Backup the binary configuration file to a TFTP server.
2. Download the special image file (4.2.4).
3. Download the 1.0.0.15 diagnostic code file. The system reboots after this step.
4. Download the 4.4 image file. The system reboots after this step.



### **Important:**

If you use Web management to upgrade your switch, close the window and refresh the browser cache before you launch EDM.

---

## Supported software and hardware capabilities

The following table summarizes the known capabilities for the Avaya Ethernet Routing Switch 2500 Series software release 4.4.

**Table 2: Supported capabilities for the Avaya Ethernet Routing Switch 2500 Series**

<b>Feature</b>	<b>Maximum number supported</b>
QoS egress queues	4
QoS filters per precedence	128 per EPIC/GPIC
QoS precedence	10 per EPIC/GPIC
Total QoS filters	(10 x 128) = 1280 per EPIC/GPIC
MAC addresses	16000
Maximum number of units in a stack	8
<b>Layer 2</b>	
VLANs	256
Spanning Tree Groups in STPG and RSTP modes	1
Multiple Spanning Tree Instances (MSTI) in MSTP mode	8
MultiLink Trunking (MLT), Link Aggregation (LAG) groups	6
Links for each MLT or LAG	4
<b>Layer 3</b>	
ARP entries (local, static & dynamic)	256 local + 256 static + 1000 dynamic
Local ARP Entries (local IP interfaces)	256
Static ARP entries	256
Dynamic ARP entries	1000
IPv4 route entries (local, static & dynamic)	256 local + 32 static + 0 dynamic
Static routes	32
Local routes	256
Management routes	4
UDP Forwarding entries	128
DHCP relay entries	256
DHCP relay forward paths	256
DHCP Server Pools	16 (one per VLAN)
DHCP Server clients per pool	254
DHCP Server clients per switch/stack	1000
<b>Miscellaneous</b>	

Feature	Maximum number supported
802.1x EAP scaling (clients for each port)	32
ADAC (IP Phones)	1 for each port 24/48 switch 192/384 for each stack
Jumbo frame support	9 K bytes
IGMP multicast groups	up to 244
802.1X (EAP) clients per port, running in MHMA	32
802.1X (EAP) clients per switch/stack	384
LLDP Neighbors per port	16
LLDP Neighbors	416/800
RMON alarms	400
RMON events	400
RMON Ethernet statistics	128 per unit
RMON Ethernet history	196 per unit

---

## Getting EDM online help files for embedded EDM

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

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

For more information about EDM, see *Avaya Ethernet Routing Switch 2500 Series Fundamentals*, NN47215-102.

---

## Downloading help files

Use the following procedure to download help files.

## Prerequisites

An available TFTP server

## Procedure Steps

You can obtain EDM help files for the embedded element manager from:

- The Avaya Web site at: <http://www.avaya.com/support>
- The software CD ROM.

To download online help files from the Avaya Web site, use the following procedure.

1. Go to the Avaya Web site at <http://www.avaya.com/support>

The Support pane appears.

2. To download software you must do one of the following:

- Click **Register** and follow the registration instructions.
- Click **Sign In** and enter your login credentials.

Once you have registered or signed in, the Support pane reappears.

3. From the list on the left side of the Support pane, click **Downloads**.

A dialog box appears.

4. In the dialog box, do one of the following:

- Enter your product name.
- Click **A-Z List**, click a letter from the selections, and select your product from the list.

The product support page appears.

5. From the list on the left side of the product support page, click **Downloads**.

The product Downloads page appears.

6. On the Downloads page, click the **Downloads** tab.

A list of available software downloads appears.

7. Click a help file to download and follow the instructions on the screen.
8. Download the help file to a TFTP server.

## Configuring the path to the help files

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

1. Open an ACLI session.
2. Go to the Global Configuration mode.
3. At the command prompt, enter the following ACLI command:

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

### EDM help file path ACLI example

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

```
edm help-file-path ERS 2500_44_Help tftp address 10.100.100.15
```

In the preceding example ERS2500\_44\_Help is a folder that contains help files and the folder is located on a TFTP server at the 10.100.100.15 address.

**Table 3: Variable definitions**

Field	Description
path name	Specifies the path name you created for EDM help files. The path name is stored in NVRAM.
TFTP address	<p>Specifies EDM TFTP server IP address. Use this address only for EDM help files. If you do not specify a TFTP server address, the system uses the address specified most recently.</p> <p> <b>Warning:</b> Because the TFTP server address is stored in NVRAM, each time the system returns to the default configuration, you must reconfigure the path to EDM online help.</p>

## Configuring the path to the help files using EDM

Use the following procedure to configure the path to the help files if you are using the embedded version of online help.

1. In the navigation tree, click **Edit**.
2. In the Edit tree, click **File System** to open the File System work area.

3. In the File System work area, click the **Help File Path** tab.
4. In the Path dialog box, enter the path to the help file storage location.  
Example, tftp://A.B.C.D./file\_name.

---

## SFP transceiver compatibility

The following table lists the SFP transceiver compatibility.

**Table 4: SFP transceiver compatibility**

Supported SFPs	Description	Minimum software version	Part number
<b>Small form factor pluggable (SFP) transceivers</b>			
1000BaseBX	1310 nm LC connector	4.3.0	AA1419069-E5
1000BaseBX	1490 nm LC connector	4.3.0	AA1419070-E5
1000BaseBX DDI	1310 nm LC connector, up to 40 km	4.3.0	AA1419076-E5
1000BaseBX DDI	1490 nm LC connector, up to 40 km	4.3.0	AA1419077-E5
1000BaseEX	1550nm LC connector up to 120 km	4.3.0	AA1419071-E5
1000BaseLX	1310 nm LC connector	4.0.0	AA1419015-E5
1000BaseLX DDI	1310 nm LC connector	4.2.0	AA1419049-E6
1000BaseSX	850 nm LC connector	4.0.0	AA1419014-E5
1000BaseSX	850 nm MT-RJ connector	4.0.0	AA1419013-E5
1000BaseSX DDI	850 nm LC connector	4.2.0	AA1419048-E6
1000BaseXD	1310nm LC connector up to 40 km	4.3.0	AA1419050-E5
1000BaseXD	1550nm LC connector up to 40 km	4.3.0	AA1419051-E5
1000BaseZX	1550nm LC connector up to 70 km	4.3.0	AA1419052-E5
1000BaseCWDM-XD	1470 nm LC connector, up to 40 km	4.0.0	AA1419025-E5
1000BaseCWDM-XD	1490 nm LC connector, up to 40 km	4.0.0	AA1419026-E5

Supported SFPs	Description	Minimum software version	Part number
1000BaseCWDM-XD	1510 nm LC connector, up to 40 km	4.0.0	AA1419027-E5
1000BaseCWDM-XD	1530 nm LC connector, up to 40 km	4.0.0	AA1419028-E5
1000BaseCWDM-XD	1550 nm LC connector, up to 40 km	4.0.0	AA1419029-E5
1000BaseCWDM-XD	1570 nm LC connector, up to 40 km	4.0.0	AA1419030-E5
1000BaseCWDM-XD	1590 nm LC connector, up to 40 km	4.0.0	AA1419031-E5
1000BaseCWDM-XD	1610 nm LC connector, up to 40 km	4.0.0	AA1419032-E5
1000BaseCWDM-ZX	1470 nm LC connector, up to 70 km	4.0.0	AA1419033-E5
1000BaseCWDM-ZX	1490 nm LC connector, up to 70 km	4.0.0	AA1419034-E5
1000BaseCWDM-ZX	1510 nm LC connector, up to 70 km	4.0.0	AA1419035-E5
1000BaseCWDM-ZX	1530 nm LC connector, up to 70 km	4.0.0	AA1419036-E5
1000BaseCWDM-ZX	1550 nm LC connector, up to 70 km	4.0.0	AA1419037-E5
1000BaseCWDM-ZX	1590 nm LC connector, up to 70 km	4.0.0	AA1419039-E5
1000BaseCWDM-ZX	1610 nm LC connector, up to 70 km	4.0.0	AA1419040-E5
1000BaseCWDM DDI	1470nm LC connector, up to 40 km	4.3.0	AA1419053-E6
1000BaseCWDM DDI	1490nm LC connector, up to 40 km	4.3.0	AA1419054-E6
1000BaseCWDM DDI	1510nm LC connector, up to 40 km	4.3.0	AA1419055-E6
1000BaseCWDM DDI	1530nm LC connector, up to 40 km	4.3.0	AA1419056-E6
1000BaseCWDM DDI	1550nm LC connector, up to 40 km	4.3.0	AA1419057-E6

Supported SFPs	Description	Minimum software version	Part number
1000BaseCWDM DDI	1570nm LC connector, up to 40 km	4.3.0	AA1419058-E6
1000BaseCWDM DDI	1590nm LC connector, up to 40 km	4.3.0	AA1419059-E6
1000BaseCWDM DDI	1610nm LC connector, up to 40 km	4.3.0	AA1419060-E6
1000BaseCWDM DDI	1470nm LC connector, up to 70 km	4.3.0	AA1419061-E6
1000BaseCWDM DDI	1490nm LC connector, up to 70 km	4.3.0	AA1419062-E6
1000BaseCWDM DDI	1510nm LC connector, up to 70 km	4.3.0	AA1419063-E6
1000BaseCWDM DDI	1530nm LC connector, up to 70 km	4.3.0	AA1419064-E6
1000BaseCWDM DDI	1550nm LC connector, up to 70 km	4.3.0	AA1419065-E6
1000BaseCWDM DDI	1570nm LC connector, up to 70 km	4.3.0	AA1419066-E6
1000BaseCWDM DDI	1590nm LC connector, up to 70 km	4.3.0	AA1419067-E6
1000BaseCWDM DDI	1610nm LC connector, up to 70 km	4.3.0	AA1419068-E6

See *Avaya Ethernet Routing Switch 2500 Series Installation*, NN47215-301 for more information.

---

## Important note on use of the two rear 1000Base-T (RJ-45) ports (all models)

The two rear facing 1000Base-T ports on all Ethernet Routing Switch 2500 Series switches are capable of supporting two different functional modes of operation. They are Stand-alone Mode and Stacking Mode operation.

In Stand-alone Mode, the rear ports can be used as normal Ethernet ports to connect a server, host or as uplink ports, and support the same configuration options as all front panel ports.

In Stacking Mode, the rear ports allow resilient stacking of up to eight Ethernet Routing Switch 2500 switches in any combination to form a single virtual switch.

 **Important:**

Stacking capability is delivered in two distinctively different ways on ERS 2500 series switches.

1. By means of software using a licensing mechanism available through the purchase of an Ethernet Routing Switch 2500 series Stacking License Kit (one license required for each switch), required for switch order codes AL2500xxx-E6.
2. By means of stack enabled versions of Ethernet Routing Switch 2500 switches where the rear ports are factory pre-enabled and configured in Stacking Mode by default and are ready to stack—with order codes AL2515xxx-E6. Stack-enabled ERS 2500 switches do not use or require a license file.

---

## Supported standards, RFCs and MIBs

The following sections list the standards, RFCs and MIBs supported in Release 4.4.

---

### Standards

The following IEEE Standards contain information pertinent to the Avaya Ethernet Routing Switch 2500 Series:

- IEEE 802.1AB (Link Layer Discovery Protocol)
- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1s (Multiple Spanning Tree Protocol—MSTP)
- IEEE 802.1w (Rapid Spanning Tree Protocol—RSTP)
- IEEE 802.1X (EAPoL)
- IEEE 802.3 (Ethernet)
- IEEE 802.3ab (Gigabit Ethernet over Copper)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3af (Power over Ethernet)
- IEEE 802.3u (Fast Ethernet)

- IEEE 802.3x (Flow Control)
- IEEE 802.3z (Gigabit Ethernet)

---

## RFCs and MIBs

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

- RFC 768 (UDP)
- RFC 783 Trivial File Transfer Protocol (TFTP)
- RFC 791 (IP)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 826 (ARP)
- RFC 854 (Telnet)
- RFC 894 (IP over Ethernet)
- RFC 951 (BootP)
- RFC 1112 (IGMPv1)
- RFC 1157 (SNMP)
- RFC 1213 (MIB-II)
- RFC 1215 SNMP Traps Definition
- RFC 1271 (RMON)
- RFC 1350 (TFTP)
- RFC 1361 Simple Network Time Protocol (SNTP)
- RFC 1573 Interface MIB
- RFC 1493 (Bridge MIB)
- RFC 1643 Ethernet MIB
- RFC 1757 (RMON)
- RFC 1769 Simple Network Time Protocol (SNTP)
- RFC 1905 SNMP
- RFC 1906 SNMP Transport Mappings
- RFC 1907 SNMP MIB
- RFC 1945 (HTTP v1.0)
- RFC 1981 (Path MTU Discovery for IPv6)

- RFC 2011 SNMP v2 MIB for IP
- RFC 2012 SNMP v2 MIB for TCP
- RFC 2013 SNMP v2 MIB for UDP
- RFC 2131 (BootP/DHCP Relay Agent)
- RFC 2132 DHCP Option 6, 43 & 60
- RFC 2138 (RADIUS)
- RFC 2236 (IGMPv2)
- RFC 2460 (Internet Protocol v6 - IPv6 - Specification)
- RFC 2461 (Neighbor Discovery for IPv6)
- RFC 2462 (Autoconfiguration of link local addresses)
- RFC 2474 Differentiated Services Support
- RFC 2570 SNMPv3
- RFC 2571 SNMP Frameworks
- RFC 2572 SNMP Message Processing
- RFC 2573 SNMPv3 Applications
- RFC 2574 SNMPv3 USM
- RFC 2575 SNMPv3 VACM
- RFC 2576 Co-existence of SNMP v1/v2/v3
- RFC 2660 HTTPS (Secure Web Server)
- RFC 2665 (Ethernet MIB)
- RFC 2674 (Q-BRIDGE-MIB)
- RFC 2737 (Entity MIBv2)
- RFC 2863 (Interfaces Group MIB)
- RFC 2865 (RADIUS)
- RFC 2866 (RADIUS Accounting)
- RFC 2869 (RADIUS Extensions)
- RFC 3046 DHCP option 82, Relay Agent Information Option
- RFC 3058 (RADIUS Authentication)
- RFC 3361 SIP Servers DHCP option 120
- RFC 3410 (SNMPv3)
- RFC 3411 (SNMP Frameworks)
- RFC 3412 (SNMP Message Processing)

- RFC 3413 (SNMPv3 Applications)
- RFC 3414 (SNMPv3 USM)
- RFC 3415 (SNMPv3 VACM)
- RFC 3416 SNMP
- RFC 3417 SNMP Transport Mappings
- RFC 3418 SNMP MIB
- RFC 3576 (RADIUS Dynamic Authorization Extensions)
- RFC 3584 Co-existence of SNMP v1/v2/v3
- RFC 4291 (IPv6 Addressing Architecture)
- RFC 4443 (Internet Control Message Protocol - ICMPv6)
- RFC 4673 (RADIUS Dynamic Authorization Server MIB)
- RFC 4675 (RADIUS Attributes for VLAN and Priority Support)
- RFC 5176 (RADIUS Dynamic Authorization Extensions)
- RFC 2819 (RMON MIB)
- RFC 4007 (Scoped Address Architecture)
- RFC 4193 (Unique Local IPv6 Unicast Addresses)
- RFC 4301 (Security Architecture for the Internet Protocol)
- RFC 5010 DHCP option 82, Relay Agent Information Option



# Chapter 4: Resolved issues

Use the information in this section to learn more about issues resolved in this release.

The following table describes the issues in previous software releases for the Ethernet Routing Switch 2500 Series that have been resolved in software release 4.4.

**Table 5: Issues resolved in ERS 2500 Series software release 4.4**

Reference Number	Description
wi00489610	MLT utilization tab is missing for EDM interface.
wi00489617	Combo ports still sends out FLP's when Auto-neg is disabled on copper interface.
wi00489721	EDM: Missing (C/S/I) type field for system logs in EDM syslog display.
<b>Resolved prior to Release 4.4</b>	
Q01874036-01	VLACP: Traffic down when multiple show commands are entered. Resolved
Q02029510	Serial connection blocked for 15 minutes on non-base when interrupting the agent download. Resolved
Q01876567-01	802.1X RFC3576: No SNMP support to enable/disable feature on interface. Resolved
Q01687454	No telnet session can be opened during VLAN display. Another session must be opened after VLAN display. Resolved.
Q01688663	The rear-ports related commands are hidden when the switch is part of a stack. Resolved.
Q01741602	Ping does not work between DUTs connected with eight links LAG in certain conditions. Resolved.
Q01507984	Currently, QoS Policy configuration (Strict, Weighted Round-Robin, Bounded Round-Robin) with corresponding Q weights and Traffic Class Priority can only be configured using the Web-based management interface. These fields should be configurable from the ACLI also. Resolved.
Q01721997	After the link on a port goes down, while several hosts are authenticated in MHMA mode on the same port. The hosts are shown in initialized state in the command output for: <code>show eapol multihost status</code> Resolved.
Q01747943	Resetting of the base unit of a stack is not recommended when a dynamically 802.3AD Trunk includes ports from the base unit. Resolved.
Q01784784	The correct MTU value for combo ports is 9216. Resolved.

## Resolved issues

Reference Number	Description
Q01776891	LLDP-MED is supported in the 4.1 release. Resolved.

# Chapter 5: Known issues and limitations

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

---

## Known issues

The following tables describe known limitations and considerations in the Avaya Ethernet Routing Switch 2500 Series software up to and including release 4.4.

**Table 6: Known issues and limitations for ERS 2500 Series Release 4.4**

Reference number WI00...	Description
831906	There is no support for configuring AAUR/DAUR in EDM
833231	Avaya recommends that you do not enable IP Source Guard on trunk ports.
833241	With the addition of IGMPv3, Any previous v1 or v2 setting will be overwritten with settings for both v1 and v2. The last ports specified will be set for both IGMPv1/ v2 Static Router Ports.
838993	The stack will intermittently be unsuccessful saving the configuration file to the TFTP server due to intra-stack communication failure.
855393	VLACP: VLACP permits the traffic flow to start after 3 consecutive packets when Timeout Type is set to "Short"
884416	In VLACP, the Timeout Type can not be changed when Fast Time and Slow Time are equal. .
886184	Attempts at very large Multi Port Configuration (MPC) in EDM will result in only partial configuration. It is recommended that fewer ports or fewer options are selected per operation.
888311	Attempts at very large Multi Port Configuration (MPC) in EDM will result in only partial configuration. It is recommended that fewer ports or fewer options are selected per operation.
896040	DHCP Server: In order to use DHCP Server, you must establish a link up in the management VLAN because DHCP Server uses the management VLAN IP address.
896045	DHCP Server: Lease time for static defined stations is infinite, regardless of the host IP pool lease time.

Reference number WI00...	Description
896050	DHCP Server: If you enable DHCP Server, IP static pools appear in the lease table.
903576	DHCP Server: In complicated setups, the ASCII configuration for DHCP is too large to reload. You must enter commands using individual lines.
904057	EAP supplicant gets IP address without authentication on a port with DHCP-Server enabled. It will not have connectivity because that is prevented by EAP on the switch.
906165	STACKING, ASSET ID: If you configure the asset ID for the current unit, the stack setting is deleted. WORKAROUND: Specify the arguments for the asset ID [stack   Unit (1–8)].
907141	If a pool has 8 IP addresses configured for any server option, for instance option 3 or 6, then you must first disable DHCP Server and then delete that pool.
908660	With DHCP Server enabled, trap and log messages may continue to be sent/written anytime a station request a new lease of an IP Pool. To stop the bsnConfigurationSavedToNvram messages from being sent out continuously during the day, it is recommended that Autosave be disabled whenever DHCP Serve is enabled. Failure to do so could cause the internal logs to fill.

**Table 7: Known issues and limitations in ERS 2500 Series up to and including release 4.3**

Reference Number	Description
Q01491509	In MSTP or RSTP, if the TxHoldCount is modified, the TxCount value is not zeroed.
Q01483088	The following error message appears when a broadcast storm occurs: (tIdt): panic: netJobAdd: ring buffer overflow!
Q01483689	The Ethernet Routing Switch 2500 Series does not forward packets to multicast address 01-00-00-00-xy-00.
Q01498529	If the PD Detect Type on an Ethernet Routing Switch 2500-PWR is set to 802.3af and Legacy, and a PoE port on the switch is connected to a non-PoE device, the status for the PoE port can appear incorrectly as InvalidPD rather than Detecting.
Q01510139	If you connect two Ethernet Routing Switch 2500-PWR Series units using PoE ports (anywhere from eight to 12 connections) and the PD Detect Type is set to 802.3 af and Legacy, after a period of minutes (maximum 3), one of the units interprets the other as a valid PD and begins delivering power through one of the PoE ports. If you then unplug the unit receiving PoE power, it remains powered and continues to forward traffic.

Reference Number	Description
Q01501869	After a Spanning Tree topology change, the entries in the MAC address table only age out after the expiration of the default aging time, rather than the forward delay time. This issue only occurs if the forward delay time is set to 4 seconds.
Q01567158	If you set up an MLT containing rear ports and combo ports, multicast and broadcast traffic travels down the first rear port instead of the lowest active MLT port.
Q01747869	<p>The number of characters that can be introduced for a password in the Web-based management login page is limited to 15, although the authentication type can be RADIUS and the password configured on the RADIUS server is greater than 15.</p> <p> <b>Important:</b> Users configured on the Radius server should not have a password longer than 15 characters.</p>
Q01754223	When configuring a DMLT on 2 or more units, Avaya recommends to use the same rate-limit settings on the units. If the rate-limit settings are different, DMLT ports could become administratively shutdown after initiating a boot session.
Q01744852	In a specific setup, first MLT link might go down after reboot/power cycle if auto-negotiation is disabled. Avaya recommends that all MLT ports should have auto-negotiation enabled.
Q01759611	After configuring RMON alarms on a stack, Avaya recommends that you do not use the renumbering units feature, because RMON alarms are not relocated to corresponding ports accordingly.
Q01760981	If a switch and a loop are connected using a link, and you create a loop on the hub, then the switch does not go in to a Forwarding State even when the loop is removed.
Q01480212	Port-mirroring mode XTX mirrors egressed traffic on the mirrored port but does not mirror control packets generated by the switch. The monitor port does not receive copies of the generated control packets that egress from the mirrored port.
Q01482942	In the ACLI Quick Start menu, if you enter a very long read-only or read-write community string (more than 32 characters), you cannot delete all of the entered characters.
Q01777899 Q01777910	When making configuration changes to the switch, allow at least 30 seconds after the last change is made before any power interruption occurs.
Q01493771	Rate limiting counts packets from the beginning of each second. When the number of packets reaches the value of the rate limit, all remaining packets are dropped until the end of the second, meaning that no packets are transmitted during the remaining interval. As a result, the packets are not evenly distributed over the course of a second. They are only sent at

Reference Number	Description
	the beginning of the second. This means that if packet counters are not perfectly synchronized with the beginning of each second, the counters can register a number of packets that does not represent the actual number of packets transmitted during that second. For example, a packet counter can register a rate limit of 5000 pps as a variable rate alternating between 2100 and 8900 pps.
Q01775878	The 'Admin Status' parameter of <b>show eapol command</b> displays the port status for hosts using an EAP client for authentication. In case of a Non-EAP clients, the status of all Non-EAP clients currently active on switch can be seen using <b>show eapol multihost non-eap-mac status</b> command.
Q01874700	If you issue the <b>show port-mirroring</b> command repeatedly right after the <b>set port-mirroring</b> command the feature state appears as enabled. Port mirroring is actually disabled, but the <b>set port-mirroring</b> command takes a while to become effective. If you issue the <b>show port-mirroring</b> command after 5-10 seconds, port mirroring appears as disabled.
Q01874770	The system sends three stack monitor traps at the same time after 1 min. 5 sec. if a unit fails (power off) with stack monitor enabled. The system does not send any other traps during this period (link up or down).
Q01876616	Logging Events Disable is ignored under Temporary Base Unit. A stack will continue to log events for all the stack units if Logging Events is set to disable under Temporary Base Unit. Workaround: Once the new unit rejoins the stack, enter the <b>logging disable</b> command once more so the configuration affects the whole stack.
Q01910550-02	If you change the stack password in stack mode, the password for the switch also changes to the stack password.
Q01921814	If you administratively disable links with IPSG configured on LACP-enabled ports, the IP filters installed by IPSG on the LACP trunk may not be removed.
Q01930298	Verify your ASCII configuration if the stack does not join after you download it. A configuration error in the file can cause the stack operation to fail.
Q01935551	To download the diagnostic code to a switch or stack, you must explicitly specify the diag field in the ACLI command.
Q01950079	The system resets the user-configurable user names when you upgrade to release 4.2 to the default values (RO, RW). The system does save the passwords when you upgrade to release 4.2.
<b>Originating in release 4.3</b>	
Q01946192	Layer 2 general: Fiber link does not take over the traffic on the combo ports if the copper link is up.

Reference Number	Description
Q02035360	EDM: If any of 3 open EDM sessions is not refreshed, a fourth session can be opened. The fourth session replaces the last unused session, which can cause one of the original 3 sessions to time out. <b>SOLUTION</b> : A maximum of 3 concurrent EDM sessions per stack is recommended.
Q02039239	IPSG: The IPSG can be enabled on up to 6 ports on an EPIC (group of 8 10/100 ports).
Q02039611	IPv6, IGMP Multicast no flood: The frames with the MAC address of the IPv6 neighbor discovery packets are dropped on both egress and ingress when IGMP Multicast no flood is enabled.
Q02046465 Q02057054	Port Mirroring: Traffic is tagged when mirrored between units in a stack.
Q02052900	IPv6: The current interface settings for the management VLAN are kept after downloading a binary configuration file.
Q02053634	EDM: you cannot reset a switch to default using EDM. <b>WORKAROUND</b> : Use the console to reset a switch to factory default.
Q02056059-01	CONSOLE: During password configuration from a Telnet session the console can be blocked until the timeout expires. <b>WORKAROUND</b> : This is expected behavior. You can reset the timeout interval from 1 to 60 minutes. The default value is 15 minutes.
Q02056133-01	EDM: Device administration using EDM can be done only if the Web server is enabled. If it is not, you can enable it using the ACLI command <b>web-server enable</b> .
Q02056594	IPv6: The IPv6 management data is kept when downgrading and restored upon upgrade.
Q02057953	QoS: You cannot create policy with DSCP remarking for IPv6 as action.
Q02058329	QoS: QoS resources taken by unrestricted interfaces are displayed incorrectly by diag.
Q02061397	EDM: When you open an EDM session, The Device Physical View does not display until the initialization process completes.
Q02062487	QoS: One extra QoS mask is consumed when you enable ARP Inspection.
Q02063936	QoS: You can configure up to 128 filters for the 10/100 ports.
Q02064299	EDM: The system displays an invalid value for QoS meter/shaper rate in capability tabs.
Q02065308	EDM: Not all IGMP groups learned are displayed for all VLANs.
Q02067109	EDM: The custom banner may not display properly when more than one space is entered back to back. <b>WORKAROUND</b> : If more than one space is required, please use CLI.

Reference Number	Description
Q02067944-01	EDM: To copy/paste cell contents you must click the source to set the edit state before you can copy the contents. <b>WORKAROUND:</b> Export table contents to a text file and copy data from the text file.
Q02081441	VLACP: When disabling VLACP globally, or per interface, the following message is logged in syslog: PortX reenabled by VLACP.
Q02083573	ASCII Config, SSH/SSL: ASCII scripts containing activation commands for SSH or SSL should be applied only after the SSH keys or SSL certificate are generated.
Q20804526	EDM: You may see unexpected sorting results when you sort columns in a table.
Q02085822	STACK: If you disable Spanning Tree Protocol (STP) on LACP ports, broadcast storms may occur until the ports form the LAG. <b>WORKAROUND:</b> It is recommended that you ensure that STP is enabled when you configure and form Link Aggregation Groups (LAGs).
Q02088293	ADAC: A maximum of 7 phones can be detected on each group of 8 ports (on a switch with default configuration). The number can decrease if other features based on hardware filters are enabled on any port from the group.
Q02089176	NetMgmt-MIB/SNMP/RMON, SSCP-Lite: In an 8 high stack PVID may not be reset on ports.
Q02090314	ASCII Configuration Generator (ACG): Some of the application-specific trap-related ACLI commands are no longer generated.
Q02091513-01	ACG, helpfile path: You must use double-backslashes when specifying a path that begins with quotes and contains a backslash.
Q02092211	EDM: Utilization values displayed in history entries will be less than expected.
Q02095930	ACLI: The ACLI command <b>mac-security snmp-trap</b> is no longer available. Please use the ACLI command <b>snmp-server notification-control</b> to set the state of the MAC Security-related notifications.
Q02097989	QoS: Two extra QoS masks are consumed on all device ports when you enable IGMP snooping on a VLAN with one or no port members.
Q02098573	EDM: If you use Firefox as your Web browser you may experience display anomalies when you open the QoS meter and System Element insertion dialogs.
Q02099605	SNMP Notification Control: The notifications state set using the <b>snmp-server notification-control</b> ACLI command is not reflected by the application-related commands.
Q02100917-01	ACLI, VLACP: There is no online help for VLACP ethertype of VLACP time-out scale commands.

Reference Number	Description
Q02108463	QoS: When QoS unicast traffic is redirected to a port on another unit (when in stack) if an if-action-extension, the packet is dropped.
Q02108492-01	802.1 software: The spanning-tree RSTP traps ACLI commands are no longer generated by the ASCII Configuration Generator. This has been replaced by the snmp-server notification-control ACLI commands.
Q02110908-01	VLAN: When attempting to display a VLAN range, the display will be interrupted when encountering a non-existent VLAN. An error message is displayed and the rest of the range is not displayed. <b>WORKAROUND:</b> Use the ACLI command <b>show vlan all</b> .
Q02111347	EDM: When you use Firefox as your Web browser the system displays an 'Unresponsive Script' warning if you hide non-editable columns in the EAPOL Multiple Port Configuration pane. You may also receive this warning message in other multiple port configuration panes where there are greater than or equal to 1000 rows of information in the table.
Q02111917	EDM, Agent: Notify-filter profile behavior is not the expected behavior. <b>WORKAROUND:</b> You must select, or deselect, the values you want to modify.
Q02111920	MetMgmt-MIG/SNMP/RMON, ACLI: Use the <b>show running-config</b> ACLI command in order to see the SNMP host-filter association.
Q02111922	NetMgmt-MIG/SNMP/RMON: The notify-filter profiles created when a stack is operating in the temporary base mode are lost upon reboot.
Q02112084	ACLI, show running-config specific command: The output of the <b>show running-config</b> command may appear to stop and start intermittently. This normal operation ensures that switch management tasks receive appropriate priority.
Q02112330	EDM: If the help file path is not configured, or is misconfigured, and multiple users try to access the online help, the help pages may not open and the system displays errors on the console.
Q02112658	EDM, Stack renumbering: If you renumber stack members then reboot the switch the following error message appears - No changes have been detected. Switches will not be renumbered.
Q02113334-02	ACLI: The PoE-trap ACLI commands are no longer available. <b>WORKAROUND:</b> Use the ACLI command <b>snmp-server notification-control</b> to set the state of the PoE-related notifications.
Q02116024	EDM: When you boot from MSTP to STPG mode, the system displays an incorrect STG ID in the VLAN table.
Q02118842	EDM: On the SSH tab, when you try to modify the TFTP Server Address field, the system generates the following error message - TftpServerInetAddress: Invalid inet address pair.

Reference Number	Description
Q02119067	Port Driver: When you use copper 1G ports, do not disable autonegotiation; use CANA for speeds less than 1000MB.
Q02119453	Port Mirroring: You are not able to mirror packets that originate from the same switch where your monitor port resides. For example, you cannot monitor ICMP ping requests originating from the switch if your monitor port resides on the same switch.
Q02119514	ACG: When you are running scripts, ensure that you create all VLANs before you add or remove ports from the newly-defined VLANs.
Q02119519	EDM: EDM will not display tables that have an apostrophe in them. If the apostrophe already exists, you will need to use ACLI for display or modifications.

---

## Known limitations

The following table lists the feature limitations in the Avaya Ethernet Routing Switch 2500 Series release 4.4.

**Table 8: Known limitations**

Reference number	Description
1	Supports only 16k MACs
2	802.1D: one Spanning Tree Group for all ports
3	Rate Limiting: settings for each box, in packets per second
4	Port Mirroring: one-to-one mirroring only
5	IP Manager: up to 10 allowed IP addresses
6	RMON: 400 alarms and events
7	VLAN: port-based, IVL only
8	IGMP: IGMPv1 and IGMPv2 supported; up to 244 Multicast Groups
9	ADAC: up to 32 devices for each port (IP Phones or other) or 16 when using only LLDP-based detection
10	802.1x NEAP: up to 32 MACs allowed for each port
11	802.1x MHSA: up to 32 MACs allowed for each each port
12	802.1x MHMA: upto 32 EAP clients allowed for each port
13	IPSG: Due to an existing Ethernet Routing Switch 2500 Series hardware limitation, you can only enable IP Source Guard on a

Reference number	Description
	maximum of six ports simultaneously out of each group of eight, no matter which operating mode, either standalone or stacking, you use. (Q01878909)
14	QoS: filters per precedence = 128 per EPIC/GPIC
15	QoS: precedence = 10 per EPIC/GPIC
16	QoS: total filters (10 x 128) = 1280 per EPIC/GPIC
17	EDM: Existing, legacy trap receiver tables cannot be viewed or configured using EDM because EDM uses the bsncNotifyControlTable to implement the Trap Web page.
18	EDM: A maximum of 3 concurrent EDM sessions per stack is recommended.
19	EDM: Expected behavior—the initial EDM startup page load time is longer than the load time for subsequent pages.
20	EDM: The QoS wizard is unavailable in Release 4.4.
21	EDM: The following pages are not supported in EDM: <ul style="list-style-type: none"> <li>• High Speed Flow Control</li> <li>• RMON Event Log</li> </ul>

