



Release Notes for Avaya Ethernet Routing Switch 4000 Series

Release 5.7
NN47205-400
Issue 10.03
November 2013

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

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

Licence types

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

Heritage Nortel Software

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

Copyright

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

Third Party Components

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

Preventing Toll Fraud

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

company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction	7
Purpose.....	7
Related resources.....	8
Support.....	9
Chapter 2: New in this release	11
Features.....	11
802.3at LLDP based discovery.....	11
802.1X-2004 support.....	11
ADAC Uplink over SPBM.....	12
802.1X Block subsequent MAC authentication.....	12
boot partial-default command.....	12
Change RADIUS Password.....	13
Default all EAP settings.....	13
EAP and NEAP separation.....	14
EAP-MD5 authentication.....	14
eapol multihost mac-max.....	14
EDM improved download support.....	15
EDM inactivity time out.....	15
Fail Open VLAN Continuity mode.....	15
FastEthernet replaced with Ethernet.....	16
Show FLASH History.....	16
Jumbo frames.....	16
Link-state tracking.....	17
List command.....	17
MAC Security Port Lockout.....	17
MLT/DMLT/LAG dynamic VLAN behavior changes.....	18
NEAP IP Phone support enhancement.....	18
NEAP not Member of VLAN.....	18
Password change via EDM.....	18
RADIUS NEAP password configurable key.....	18
Remote Switch Port ANalyzer.....	19
Remove NSNA.....	19
RO User access to telnet and SSH.....	19
Run Scripts.....	19
SFTP License and DHCP external support.....	20
show ip netstat.....	20
Show VLAN interface verbose command.....	20
SLA Monitor.....	20
SPBM.....	21
Syslog Support for 802.1X/EAP/NEAP/UBP.....	21
Trace Support for 802.1X.....	21
User Based Policies.....	22
Other changes.....	22
Chapter 3: Important notices	23

Supported software and hardware capabilities.....	23
Filter, meter and counter resources.....	25
File names for this release.....	27
Supported traps and notifications.....	29
Supported Web browsers for Enterprise Device Manager.....	29
Upgrading Software.....	29
Effects of Upgrade on Unified Authentication.....	32
Effects of Upgrade on SNMP Trap Notifications.....	33
Updating switch software.....	35
General software upgrade instructions.....	36
Changing switch software in ACLI.....	36
Job aid—download command parameters.....	37
Changing switch software in EDM.....	38
Job aid—File System screen fields.....	39
Setting IP parameters with the ip.cfg file on a USB memory device.....	41
Hardware and software compatibility.....	44
XFP, SFP and SFP+ Transceiver Compatibility.....	44
Supported standards, RFCs and MIBs.....	48
Standards.....	48
RFCs and MIBs.....	49
IPv6 specific RFCs.....	51
Chapter 4: Resolved issues.....	53
Chapter 5: Known Issues and Limitations.....	57
Known Issues and Limitations for Release 5.7.....	57
Known Issues and Limitations for Releases Prior to Release 5.7.....	60
IPv6 limitations.....	76

Chapter 1: Introduction

Purpose

This document describes new features, hardware, upgrade alerts, known and resolved issues, and limitations for Avaya Ethernet Routing Switch 4000 Series, Software Release 5.7.

The following switch models are supported:

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

Configurations can vary from a stand-alone switch to a stack of up to 8 switches. A stack can consist of any combination of switches. One of the benefits of operating Avaya Ethernet Routing Switch 4000 Series switches in a stack is management efficiency; a stack is managed with a single IP address and software is available as a single image across all models.

Related resources

Documentation

For a list of the documentation for this product, see *Documentation Reference for Avaya Ethernet Routing Switch 4000 Series*, NN47205–101.

Training

Ongoing product training is available. For more information or to register, see <http://avaya-learning.com/>.

Enter the course code in the **Search** field and click **Go** to search for the course.

Course code	Course title
8D00020E	Stackable ERS and VSP Products Virtual Campus Offering

Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to <http://support.avaya.com>, select the product name, and check the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to <http://www.youtube.com/AvayaMentor> and perform one of the following actions:
 - Enter a key word or key words in the Search Channel to search for a specific product or topic.
 - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

*** Note:**

Videos are not available for all products.

Searching a document collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
 2. Navigate to the folder that contains the extracted files and open the file named *<product_name_release>.pdx*, for example, *ers4000_5.7x.pdx*.
 3. In the Search dialog box, select the option **In the index named *<product_name_release>.pdx***.
 4. Enter a search word or phrase.
 5. Select any of the following to narrow your search:
 - Whole words only
 - Case-Sensitive
 - Include Bookmarks
 - Include Comments
 6. Click **Search**.

The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance ranking.
-

Support

Visit the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release

notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: New in this release

The following sections detail what is new in *Avaya Ethernet Routing Switch 4000 Series Release Notes* — Software Release 5.7.

Features

See the following sections for information about the new features.

802.3at LLDP based discovery

ERS 4000 Series PWR+ devices support the IEEE 802.3at-2009 standard for a Link Layer Discovery Protocol (LLDP) configuration with a Powered Device (PD). The LLDP support for PoE+ is added by extending the existing standard LLDP DOT3 Power via MDI TLV defined by the IEEE 802.1ab with the new fields and values defined in the IEEE 802.3at-2009 standard. Information for power negotiation between PD and Power Sourcing Equipment (PSE) is described in Power via MDI, which is the optional TLV.

The PoE PD communicates through the Data Link Layer (DLL) classification instead of Physical Layer (high power mode). Hence, the PoE+ capable devices can deliver power greater than 15.4 watts for each port.

You can configure the PoE PD detection type (802.3at or 802.3at_and_legacy) to support a DLL classification for communication. The Data Link Layer classification provides finer power resolution and the ability for PSE and PD to participate in dynamic power allocation. The allocated power to the PD can change one or more times during PD operation.

 **Note:**

This feature is available only on the ERS 4000 series PWR+ models.

For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500.

802.1X-2004 support

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

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

ADAC Uplink over SPBM

ADAC Uplink over SPBM adds support for SPBM in ADAC, allowing ADAC to have the uplink over SPBM instead of an uplink port.

With this feature, ADAC can use an I-SID (that you associate with the ADAC Voice-VLAN) instead of a classical uplink-port. In this situation, ADAC can be enabled without the existence of a real uplink-port, and without the need of auto-configuring this uplink-port, therefore without auto-adding it to the Voice-VLAN.

For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4000 Series*, NN47205-501.

802.1X Block subsequent MAC authentication

Prior to Release 5.7, in Multiple Host with Multiple Authentication (MHMA) mode, if a station successfully authenticates, the switch places the port in the RADIUS-assigned VLAN that corresponds to that station's login credentials. If a second station properly authenticates on that same port, the switch ignores the RADIUS-assigned VLAN and the user is placed in the same VLAN as the first successfully authenticated station, creating a potential security risk. This feature enhancement provides an option to the administrator to either use the current implementation or block the subsequent MAC authentications if the RADIUS-assigned VLAN is different than the first authorized station's VLAN.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

boot partial-default command

Use the `boot partial-default` command to restore the switch to factory default configuration without losing the IP and license information, and passwords for console and Telnet/WEB.

For more information about the configuration, see *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500.

Change RADIUS Password

Remote users can change their account passwords when RADIUS is configured and enabled in your network. Once you configure RADIUS servers in your network to provide centralized authentication, authorization and accounting for network access, you can enable the MS-CHAPv2 encapsulation method, which permits the changing of the RADIUS password for user accounts.

 **Note:**

Change RADIUS password is available only in secure software builds.

Change RADIUS password is disabled by default.

If you enable RADIUS encapsulation ms-chap-v2, when an account password expires the RADIUS server reports the expiry during the next logon attempt and the system prompts you to create a new password. Also, you can change your RADIUS password before expiry using ACLI. To use change RADIUS password you must have:

- at least one configured and reachable RADIUS server in your network
- configured RADIUS encapsulation ms-chap-v2

Change RADIUS password is compatible with RADIUS password fallback.

Configuration for the change RADIUS password feature save in both the binary and ASCII configuration files.

For more information about the configuration, see *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500 and *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

Default all EAP settings

The default `eap-all` command resets all the EAP settings globally and for each port.

The global command defaults the following settings:

- EAP state
- Fail Open VLAN
- VoIP VLAN
- Allow Port Mirroring
- All Multihost settings
- MultiVLAN

- User Based Policies
- NEAP User Based Policies

Per interface command defaults the following:

- All EAP standard related settings
- All multihost settings
- Guest VLAN settings

 **Note:**

Per interface command can be used on all ports or only on a desired range of ports.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

EAP and NEAP separation

The EAP/ NEAP separation command allows you to disable EAP clients without disabling NEAP clients.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

EAP-MD5 authentication

With EAP-MD5 authentication, the RADIUS NEAP password is set with MD5 based encryption.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

eapol multihost mac-max

The `eapol multihost mac-max` command restricts the maximum number of EAP and NEAP clients allowed for each port.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

EDM improved download support

EDM displays the following status messages while downloading a software:

- Software download progress percentage to indicate the time taken to download the software to the switch
- Transferring download progress percentage to indicate the time taken to transfer the software to stack units.
- Programming percentage to indicate the time taken to write the software on the switch.
- If you are downloading software using `NoReset` option, the Status field is updated to "success" after software download.
- Estimated remaining time until the EDM interface will be operational again, after switch reboot. The EDM tries to reconnect to the switch after the estimated time. If it is not able to reconnect immediately, the estimated reattempting time is displayed. For example, the time taken to reconnect the switch can be 30 seconds.

For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500.

EDM inactivity time out

A session becomes inactive if there is no interaction with the EDM interface for more than 15 minutes. After the session becomes inactive, you must login again with your user name and password.

Using the CLI command `edm inactivity-timeout`, you can configure the time period for which an EDM session remains active.

For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500.

Fail Open VLAN Continuity mode

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

Current Avaya ERS Stackable switches provide two modes of operation for EAP/NEAP clients when the RADIUS Server is unreachable. In this standard mode of operation, the clients are moved back to the default VLAN and policies if re-authentication occurs and the RADIUS server is not reachable. In the Fail Open Continuity Mode, when an EAP or NEAP client is re-authenticated and the RADIUS server is not reachable, the switch maintains the client in the currently RADIUS assigned VLAN and any applicable policies.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

FastEthernet replaced with Ethernet

The keyword FastEthernet is replaced with Ethernet in all the ACLI commands. For compliance, the old commands containing FastEthernet keyword are hidden, and you can configure using the keyword.

 **Note:**

ASCII configurations from a release with “FastEthernet replaced with Ethernet” feature activated cannot be used to configure a setup that does not support this feature.

Show FLASH History

The FLASH history provides the current status of the FLASH device. Use the `show flash history` command to view the FLASH writes and erase history on a standalone unit or stack. The FLASH history does not record programming done from the diagnostics or bootloader. FLASH history is stored in system FLASH. The data does not get corrupted during an upgrade or downgrade. FLASH History is automatically enabled and does not require any configuration.

For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500.

Jumbo frames

A jumbo frame is an Ethernet frame that is larger than 1518 bytes. Following are the benefits when the jumbo frames are enabled:

- Each frame carries a larger payload as the header sizes remain the same.
- There are fewer interrupts on the server due to less frames and a smaller CPU load.
- Larger frames provide better buffer utilization and forwarding performance in switches.

By default, the jumbo frames are enabled. The default frame size is 9216 bytes. When jumbo frames are disabled, the frame size is 1518.

For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500.

Link-state tracking

Link-state tracking (LST) binds the link state of multiple interfaces. The Link-state tracking feature identifies the upstream and downstream interfaces. Interfaces connected to servers are referred to as downstream interfaces, and interfaces connected to distribution switches and network devices are referred to as upstream interfaces. In a link-state group, these interfaces are bundled together and the downstream interfaces are bound to the upstream interfaces.

For example, in an application, link-state tracking can provide redundancy in the network with two separate switches or stacks when used with server NIC adapter teaming. If interface 1 goes down on either switch, the server continues to send traffic through interface 2 and the traffic is dropped. If interfaces 1 and 2 are coupled in a link-state group (as upstream and downstream ports respectively), when interface 1 is unavailable, interface 2 is disabled prompting the server to choose the other path as target.

For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500.

List command

The list command lists all the command groups from each CLI mode and also displays the CLI syntax of each command.

The following commands can be used in Privileged EXEC mode:

- `show cli list`— displays the CLI command groups of each mode
- `show cli list verbose`— displays the syntax of each CLI command

For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4000 Series*, NN47205-102.

MAC Security Port Lockout

MAC Security Port Lockout feature excludes specific ports from MAC-based security. You can use this feature to simplify switch operations and prevent accidental loss of network connectivity caused by improper MAC security settings.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

MLT/DMLT/LAG dynamic VLAN behavior changes

A warning message appears when you try to remove all the VLANs on an active MLT/DMLT/LAG. The message does not appear when you try to remove multiple VLANs. Following is the warning message:

```
Warning: you are about to remove all VLANs from the active trunk
group, doing so could cause loss of connectivity to the switch. Are
you sure you want to continue <Y/N>?
```

For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500.

NEAP IP Phone support enhancement

NEAP IP Phone support is enhanced to recognize the following Avaya handset models through DHCP signature: 9611G, 9621,9641,9610, 9620L,9620C, 9630G,9650G.

NEAP not Member of VLAN

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

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

Password change via EDM

This feature provides the ability to change the switch password through EDM. This capability must be enabled if the switch is running on HTTPS or the secure image.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

RADIUS NEAP password configurable key

RADIUS NEAP password includes a configurable key string in addition to IP address, MAC address, and port number.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

Remote Switch Port ANalyzer

Remote Switch Port ANalyzer (RSPAN), also known as Remote Port Mirroring, enhances port mirroring by enabling mirroring traffic to be sent to one or more switches or stacks on the network using an intermediate VLAN for forwarding the mirrored traffic.

For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4000 Series*, NN47205-502.

Remove NSNA

From Release 5.7, ERS 4000 series does not support NSNA.

RO User access to telnet and SSH

You can access telnet and SSH commands with read-only permissions. In previous software releases, the telnet and SSH commands required only read-write permissions.

For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500 and *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

Run Scripts

According to Avaya best practices for converged solutions, you can use the scripts to configure the parameters for an Avaya stackable Ethernet Switch. The scripts can be executed in a default or verbose mode.

In the automated or non-verbose mode, the switch is configured using predetermined parameter values. In the verbose mode, the script guides you to configure the parameters where the values must be provided as inputs when the script is executed.

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

For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500.

SFTP License and DHCP external support

You can download the license file using Secure File Transfer Protocol (SFTP). You can also transfer DHCP external save file to switch or from switch using SFTP.

For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4000 Series*, NN47205-102 and *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

show ip netstat

The `show ip netstat` command displays the IPv4 socket information.

For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500.

Show VLAN interface verbose command

The `show vlan interface verbose` command displays VLAN, PVID, and port information associated with a port.

For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4000 Series*, NN47205-501.

SLA Monitor

ERS 4000 R5.7 supports SLA Mon™ Agent which provides network quality of service (QoS) monitoring and DSCP monitoring capabilities. R5.7 supports the ability to perform QoS and DSCP tests via CLI between any two Networking devices with SLA Mon™ Agents without need for an SLA Mon™ server. In addition, R5.7 supports secure agent-server communication through certificate-based authentication and encrypted agent-server communication secure communications, and is intended to interoperate with the Avaya Diagnostic Server R2.0 when it releases. Avaya Diagnostic Server will provide network-wide QoS and DSCP monitoring, along with graphical display, alarms and alerts, trend analysis, and logging.

For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4000 Series*, NN47205-502.

For more information about the Avaya diagnostic Server, see Avaya Sales Portal under Support Advantage.

SPBM

Shortest Path Bridging MAC (SPBM) is a next generation virtualization technology that revolutionizes the design, deployment and operations of Ethernet networks. SPBM enables massive scalability while simultaneously reducing the complexity of the network.

Avaya networking products allow virtualization services at both layer 2 and layer 3, referred to as L2VSN and L3VSN. The Avaya Ethernet Switch 4800 is capable of providing L2VSN support connecting traditional Ethernet networks to an SPBM enabled network core, the ERS 4800 functions as a Backbone Edge Bridge. The 5.7 release introduces L2VSN capabilities to the ERS 4800 product, whereas SPBM support is exclusive to the ERS 4800 and stacks of ERS 4800. The L3 (e.g. OSPF) features of the ERS 4800 cannot be supported simultaneously with SPBM, they are mutually exclusive.

Avaya ERS 4800 Series supports the IEEE 802.1aq standard of SPBM, which allows for larger Layer 2 topologies and permits faster convergence.

 **Note:**

SPBM is not supported on the ERS 4500 series or hybrid stacks of ERS 4500 and ERS 4800.

For more information regarding configuration and caveats using SPBM with release 5.7, see *Configuring Avaya VENA Fabric Connect on Avaya Ethernet Routing Switch 4000 Series*, NN47205-507.

Syslog Support for 802.1X/EAP/NEAP/UBP

Syslog messages for the various states of 802.1X/EAP/NEAP/UBP authentications are introduced to allow more thorough troubleshooting.

The log messages include the following information:

- Authentication time
- MAC authentication success or failure
- IP address associated with MAC authentication
- VLAN and UBP assignment

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

Trace Support for 802.1X

The trace command supports 802.1X/EAP in four levels for each module or application apart from supporting various other applications (OSPF, RIP, SMLT, IPMC, IGMP, and PIM) from

previous releases. All the previous levels of trace are supported (Very Terse, Terse, Verbose, and Very Verbose). If higher levels are requested, more information is displayed.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

User Based Policies

You can configure the Ethernet Routing Switch 4000 Series to manage access with User Based Policies (UBP). UBP revolves around the User Policy Table supporting multiple users for each interface. User data is provided through interaction with Extensible Authentication Protocol (EAP) and is maintained in the User Policy Table. You can associate a user with a specific interface, user role combination, user name string, and optionally user group string. You can also associate each user with session information. Session data maintains state information for each user. The information includes the session identifier and start time.

For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4000 Series*, NN47205-504 and *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

Other changes

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

The following documents are added for ERS 4000 Release 5.7:

- *Locating Documentation and Regulatory Reference for Avaya Ethernet Routing Switch 4000 Series*, NN47205-100
- *Quick Start Configuration for Avaya Ethernet Routing Switch 4000 Series*, NN47205-104
- *ACLI Commands Reference for Avaya Ethernet Routing Switch 4000 Series*, NN47205-105
- *Quick Installation of Avaya Ethernet Routing Switch 4000 Series*, NN47205-302
- *Installation Job Aid (English) for Avaya Ethernet Routing Switch 4000 Series*, NN47205-303
- *Configuring Avaya VENA Fabric Connect on Avaya Ethernet Routing Switch 4000 Series*, NN47205-507

Chapter 3: Important notices

The following sections provide important notices.

Supported software and hardware capabilities

The following table lists supported software and hardware scaling capabilities in Avaya Ethernet Routing Switch 4000 Series Software Release 5.7. 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	8,192
Stacking bandwidth (full stack of 8 units)	Up to 384 Gbps
QoS precedence	8 per ASIC
QoS rules per ASIC	128 rules per precedence
Maximum number of units in a stack	8
Maximum number of Port Mirroring Instances	4
Layer 2	
Concurrent VLANs	1,024
Supported VLAN IDs	1 - 4094 (0 and 4095 reserved; 4001 reserved by STP; 4002-4008 reserved by multiple STP groups)
Protocol VLAN types	7
Multi-Link Trunking (MLT), Distributed Multi-Link Trunking (DMLT), and Link Aggregation (LAG) groups	32
Maximum MAC Learning rate on an MLT trunk	500 new MAC addresses per second
Links or ports for MLT, DMLT or LAG	8
Static MAC Addresses	1,024

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

Feature	Maximum number supported
802.1x (NEAP) clients per switch/stack	384
802.1x (EAP & NEAP) clients per switch/stack	768
Maximum RADIUS Servers	2
Maximum 802.1X EAP Servers	2
Maximum 802.1X NEAP Servers	2
Maximum RADIUS/EAP/NEAP Servers	6
IPFIX number of sampled flows	100,000
LLDP Neighbors per port	16
LLDP Neighbors	800
RMON alarms	800
RMON events	800
RMON Ethernet statistics	110
RMON Ethernet history	249
Link State Tracking: Instances	***
Port Mirroring Instances	4
Port Mirroring: RSPAN VLANs	4
Port Mirroring: RSPAN destinations	4 per switch
SPB operational mode	Standalone or stack of up to 8 units
SPB nodes per region	250
SPB (IS-IS) adjacencies per node	4
SPB Customer VLANs (C-VLANs) per node	500
SPB ISIDs per node	500
SPB Switched UNIs	500
Number of B-VLANs	2
Number of ISIS interfaces per node	4

Filter, meter and counter resources

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

*** Note:**

Filters will use the highest available precedence.

Table 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
DHCP Relay	L3 mode	0	0	0	0	0
DHCP Snooping		0	0	0	2	1
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
	Untrusted					
QoS	Precedence 2	1	0	1	0	0
	Precedence 1	1	0	1	0	0
QoS	Unrestricted	0	0	0	0	0
UDP Forwarding		0	0	0	1	1
OSPF		0	0	0	3	0
RIP		0	0	0	1	0
IPFIX		0	0	0	1	1
SLPP Guard		0	0	0	1	1


File names for this release

File names for release 5.7

The following table describes the Avaya Ethernet Routing Switch 4000 Series, Software Release 5.7 software files. File sizes are approximate.

Table 3: Software Release 5.7 components

Module or File Type	Description	File Name	File Size (bytes)
Standard Runtime Software Image	Standard image for the Avaya Ethernet Routing Switch 4000 Series	4500_570008.img	10,120,272
Secure Runtime Software Image	Secure image for the Avaya Ethernet Routing Switch 4000 Series	4500_570009s.img	10,380,344
Diagnostic Software Image	4500 diagnostic image (except 4500-PWR+ models)	4500_5303_diag.bin	1,589,514
	4000 diagnostic image (4500-PWR+ and 4800 models)	4000_57001_diag.bin	1,934,097
	4000 combination diagnostic image (all 17 models)	4000_57001_combodiag.bin	3,523,611
PoE Firmware	PoE Firmware for ERS 4500 (4526T-PWR, 4550T-PWR, 4524GT-PWR, 4526GTX-PWR, 4548GT-PWR with 'Nortel' logo)	4500_PoE_400.img	77,766
	PoE Firmware for ERS 4500-PWR (4526T-PWR, 4550T-PWR, 4524GT-PWR, 4526GTX-PWR, 4548GT-PWR HW with 'Avaya' logo)	4500_PoE_400b15.img	77,923
	<p> Note: From Release 5.6.2, when the firmware image is provided, the software detects and matches the correct firmware with the</p>		

Module or File Type	Description	File Name	File Size (bytes)
	hardware. For example, enter 4500_PoE_400.img and then, enter 4500_PoE_400b15.img, the correct firmware is matched with the hardware.		
PoE+ Firmware	PoE+ Firmware for 4526T-PWR+, 4550T-PWR+, 4826GTS-PWR+, 4850GTS-PWR+	4000_PoEplus_410B4.bin	16,384
Bootloader	Bootloader image for 4500-PWR+ and 4800 models	4000_56108_boot.bin	322,522
<p> Note:</p> <p>The bootloader software is listed for completeness and is factory installed on new revision 10 hardware, there is no requirement to update the bootloader.</p>			
Enterprise Device Manager Help Files	Help files required for Avaya Ethernet Routing Switch 4000	4000_570_EDMhelp.zip	4,366,657
Enterprise Device Manager Plug-in	Avaya Ethernet Routing Switch 4000 Enterprise Device Manager plug-in for Configuration and Orchestration Manager	4000_570_EDMplugin.zip	5,335,349
Software Release 5.7 Management Information Base (MIB) Definition Files	MIB definition files	Ethernet_Routing_Switch_4000_MIBs_5.7.0.zip	2,438,539
Demonstration License	Demonstration License	4000_570_Demo.lic	420

 **Note:**

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

Supported traps and notifications

For information about SNMP traps generated by the Avaya Ethernet Routing Switch 4000 Series, see *Troubleshooting Avaya Ethernet Routing Switch 4000 Series*, 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. For higher versions, you must use Internet Explorer in compatibility mode.
- Mozilla Firefox version 23.0

For more information about EDM, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4000 Series*, NN47205-102.

Upgrading Software

To upgrade to the new software release 5.7, Avaya recommends that you first verify or upgrade the diagnostics image. For ERS 4500 models (excluding the 4526T-PWR+ and 4550T-PWR+), you are recommended to use version 5.3.0.3 of the diagnostics. For all 4800 as well as the 4526T-PWR+ and 4550T-PWR+ models, use the 5.6.2.01 diagnostics. Once the diagnostics image is verified or updated, you can then upgrade the agent version to release 5.7.

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
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

Important notices

Image	Location
5.3.0.3 Diagnostic Image	Diagnostic image released in 5.4
5.3.0.3 Diagnostic Image	Diagnostic image released in 5.5
5.3.0.3 Diagnostic Image for the following units: 4524GT, 4524GT-PWR, 4526FX, 4526GTX, 4526GTX –PWR, 4526T, 4526T-PWR, 4548GT, 4548GT-PWR, 4550T, 4550T-PWR	Diagnostic image released in 5.6
5.6.0.15 Diagnostic Image for the following units: 4550T-PWR+, 4526T-PWR+, 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+	Diagnostic image released in 5.6
Combo 5.6.0.15 Diagnostic Image that is a combination between 5.3.0.3 and 5.6.0.15 and can be downloaded on all units	Diagnostic image released in 5.6
5.3.0.3 Diagnostic Image for the following units: 4524GT, 4524GT-PWR, 4526FX, 4526GTX, 4526GTX –PWR, 4526T, 4526T-PWR, 4548GT, 4548GT-PWR, 4550T, 4550T-PWR	Diagnostic image released in 5.6.1
5.6.1.18 Diagnostic Image for the following units: 4550T-PWR+, 4526T-PWR+, 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+	Diagnostic image released in 5.6.1
Combo 5.6.1.18 Diagnostic Image that is a combination between 5.3.0.3 and 5.6.1.18 and can be downloaded on all units	Diagnostic image released in 5.6.1
5.3.0.3 Diagnostic Image for the following units: 4524GT, 4524GT-PWR, 4526FX, 4526GTX, 4526GTX –PWR, 4526T, 4526T-PWR, 4548GT, 4548GT-PWR, 4550T, 4550T-PWR	Diagnostic image released in 5.6.2
5.6.2.01 Diagnostic Image for the following units: 4550T-PWR+, 4526T-PWR+, 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+	Diagnostic image released in 5.6.2
Combo 5.6.2.01 Diagnostic Image that is a combination between 5.3.0.3 and 5.6.2.01 and can be downloaded on all units	Diagnostic image released in 5.6.2
5.3.0.3 Diagnostic Image for the following units: 4524GT, 4524GT-PWR, 4526FX, 4526GTX, 4526GTX –PWR, 4526T, 4526T-PWR, 4548GT, 4548GT-PWR, 4550T, 4550T-PWR	Diagnostic image released in 5.6.3

Image	Location
5.6.2.01 Diagnostic Image for the following units: 4550T-PWR+, 4526T-PWR+, 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+	Diagnostic image released in 5.6.3
Combo 5.6.2.01 Diagnostic Image that is a combination between 5.3.0.3 and 5.6.2.01 and can be downloaded on all units	Diagnostic image released in 5.6.3
5.3.0.3 Diagnostic Image for the following units: 4524GT, 4524GT-PWR, 4526FX, 4526GTX, 4526GTX –PWR, 4526T, 4526T-PWR, 4548GT, 4548GT-PWR, 4550T, 4550T-PWR	Diagnostic image released in 5.7
5.7.0.01 Diagnostic Image for the following units: 4550T-PWR+, 4526T-PWR+, 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+	Diagnostic image released in 5.7
Combo 5.7.0.01 Diagnostic Image that is a combination between 5.3.0.3 and 5.7.0.01 and can be downloaded on all units	Diagnostic image released in 5.7

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

! Important:

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

! Important:

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

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

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

Use the following procedure to upgrade the Agent Image from release 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.6.1, 5.6.2 or 5.6.3 to release 5.7:

Upgrading Agent Image from release 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.6.1, 5.6.2 or 5.6.3 to release 5.7

1. Upgrade the diagnostic image from the earlier release to release 5.3.0.3 diagnostic image.
2. Upgrade the agent image from release 5.0, 5.1, 5.2, , 5.3, 5.4, 5.5, 5.6, 5.6.1, 5.6.2 or 5.6.3 to release agent image 5.7.

Warning:

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

Effects of Upgrade on Unified Authentication

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

The unified authentication mechanism approach simplifies the design: using the current 'cli password' and 'username' commands the same set of read-write/read-only username and passwords and authentication type is applied to a stack as well as each standalone switch. The switch obsoletes and clears the switch passwords and username; so that when the unit is operating in either standalone or stacked mode it always uses what was previously designated as the stack password and username.

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

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

The following message appears in system log :

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

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

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

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

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

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

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

Known limitations

For a standalone unit with an switch IP address set but no stack IP address set, if RADIUS or TACACS+ authentication is desired, the command `cli password serial/telnet radius/tacacs` will only set this for the standalone operation (and the stack mode will be left at type local). After a reboot the stack credentials will overwrite switch credentials.

Workaround: To avoid this case, Avaya recommends setting a stack IP address (even on standalone operating mode) before setting authentication type.

Effects of Upgrade on SNMP Trap Notifications

Important:

A new notification control mechanism was introduced with Release 5.4.0 . If you upgrade from an earlier release, all notifications are enabled in Release 5.7, regardless of whether you disabled them prior to the upgrade. When you upgrade from Release 5.6.3 to Release 5.7 the switch remembers the prior enabled or disabled state of notifications.

You can use the following procedures to restore trap functionality.

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

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

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

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

To reconfigure traps, use the following EDM procedure:

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

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

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

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

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

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

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

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

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

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

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

To set the Notification Type per receiver, use the following ACLI procedure:

1. From the global configuration prompt, enter the following command:

```
snmp-server notify-filter TestFilter +org
```

2. From the global configuration prompt, enter the following command:

```
snmp-server notify-filter TestFilter -linkDown
```

3. From the global configuration prompt, enter the following command:

```
snmp-server notify-filter TestFilter -linkUp
```

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

- From the global configuration prompt, enter the following command:

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

To enable or disable the Notification Type per device, use the following ACLI procedure:

1. From the global configuration prompt, enter the following command:

```
no snmp-server notification-control linkDown
```

2. From the global configuration prompt, enter the following command:

```
no snmp-server notification-control linkUp
```

Updating switch software

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

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

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

OR

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

See the following sections for details about updating switch software:

- [General software upgrade instructions](#) on page 36
- [Changing switch software in ACLI](#) on page 36
- [Changing switch software in EDM](#) on page 38

General software upgrade instructions

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

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

Changing switch software in ACLI

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

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

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

3. Press `Enter`.

The software download occurs automatically without user intervention. This process deletes the contents of the FLASH memory and replaces it with the desired software image.

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

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

! Important:

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

Job aid—download command parameters

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

Table 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 or tftp and sftp parameters are mutually exclusive; you can execute only one at a time.
tftp address <ipv6 address> <ipv4 address>	The IPv4 or IPv6 address of the TFTP server you use. The address <ipv6_address> <ipv4_address> parameter is optional and if you omit it, the switch defaults to the TFTP server specified by the <code>tftp-server</code> command.
sftp address <ipv6 address> <ipv4 address>	The IPv4 or IPv6 address of the SFTP server you use. The address <ipv6_address> <ipv4_address> parameter is optional and if you omit it, the switch defaults to the SFTP server specified by the <code>sftp-server</code> command. When using SFTP, the username parameter can be utilized. Note: SFTP transfer is only possible when the switch/stack is running the secure software image.
usb [unit <unit number>]	Specifies that the software download is performed using a USB Mass Storage Device and the front panel USB port. Use the unit number parameter to specify which switch contains the USB in a stack.
image <image name>	The name of the software image to be downloaded from the TFTP/SFTP server or USB Mass Storage Device.
image-if-newer <image name>	This parameter is the name of the software image to be downloaded from the TFTP/SFTP server or USB Mass Storage Device if it is newer than the currently running image.

Parameter	Description
diag <image name>	The name of the diagnostic image to be downloaded from the TFTP/SFTP server or USB Mass Storage Device.
poe_module_image <image name>	The name of the Power over Ethernet plus firmware to be downloaded from the TFTP/SFTP server or USB Mass Storage Device. This option is available only for 4000 Series switches that support Power Over Ethernet plus.
no-reset	This parameter forces the switch to not reset after the software download is complete.
username <username> [password]	Specifies the username and optionally the password which can be used when connecting to the SFTP server. No password is required if DSA or RSA keys have been appropriately configured.

Changing switch software in EDM

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

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

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

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

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

 **Important:**

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

Job aid—File System screen fields

The following table describes the File System screen fields.

Table 6: File System screen fields

Field	Description
TftpServerInetAddress	Indicates the IP address of the TFTP or SFTP* server on which the new software images are stored for download.
TftpServerInetAddressType	Indicates the type of TFTP or SFTP* server address type: <ul style="list-style-type: none"> • IPv4 • IPv6
BinaryConfigFileName	Indicates the binary configuration file currently associated with the switch. Use this field when you work with configuration files; do not use this field when you download a software image.
BinaryConfigUnitNumber	When in standalone mode, and loading a binary configuration file that was created from a stack, this object specifies the unit number of the portion of the configuration file to be extracted and used for the standalone unit configuration. If this value is 0, it is ignored.
ImageFileName	Indicates the name of the image file currently associated with the switch. If needed, change this field to the name of the software image to be downloaded.
FwFileName (Diagnostics)	The name of the diagnostic file currently associated with the switch. If needed, change this field to the name of the diagnostic software image to be downloaded.
UsbTargetUnit	Indicates the unit number of the USB port to be used to upload or download a file. A value of 0 indicates download is via TFTP; a value of 9 indicates a standalone switch and a value of 10 indicates SFTP* server.
Action	This group of options represents the actions taken during this file system operation. The options applicable to a software download are

Field	Description
	<ul style="list-style-type: none"> • dnldConfig: Download a configuration to the switch. • dnldConfigFromSftp: Download a configuration to switch from the SFTP Server*. • dnldConfigFromUsb: Download a configuration to switch using the front panel USB port. • dnldFw: Download a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. • dnldFwFromSftp: Download a new diagnostic software image to the switch from the SFTP server. This option replaces the image regardless of whether it is newer or older than the current image*. • dnldFwFromSftpNoReset: Download a new diagnostic software image to the switch from the SFTP server. This option replaces the image regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset*. • dnldFwFromUsb: Download a new diagnostic software image to the switch from the front panel USB port. This option replaces the image regardless of whether it is newer or older than the current image. • dnldFwNoReset: Download a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset. • dnldImg: Download a new software image to the switch. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. • dnldImgFromSftp: Download a new software image to the switch from the SFTP server. This option replaces the image regardless of whether it is newer or older than the current image*. • dnldImgFromSftpNoReset: Download a new software image to the switch from the SFTP server. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset*.

Field	Description
	<ul style="list-style-type: none"> • dnldImgFromUsb: Download a new software image to the switch using the front panel USB port. This option replaces the image regardless of whether it is newer or older than the current image. • dnldImgIfNewer: Download a new software image to the switch only if it is newer than the one currently in use. • dnldImgNoReset: Download a new software image to the switch. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset. • upldConfig: Upload a configuration to the switch from a designated location. • upldConfigToSftp: Upload binary config to SFTP server*. • upldConfigToUsb: Upload binary config to USB port • upldImgToUsb: Upload image to USB port
Status	<p>Display the status of the last action that occurred since the switch last booted. The values that are displayed are</p> <ul style="list-style-type: none"> • other: No action occurred since the last boot. • inProgress: The selected operation is in progress. • success: The selected operation succeeded. • fail: The selected operation failed.

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

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

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

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

The following table describes the ip.cfg file parameters:

Table 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: ers4000/4000_5.3.0.34.bin
USBascii <string>	Specifies the file name of the ASCII configuration file to load from the USB device. Example: customer1.cfg
USBagent <string>	Specifies the file name of the runtime agent image to load from the USB device. Example: ers4000/4000_563024.img
NEXTIP, NEXTMask, and NEXTGateway	Specifies IP addresses, network mask and gateway to be used once the switch is rebooted.

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

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

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

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

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

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

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

 **Important:**

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

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

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

Press **CTRL** and **y** keys together.

Two possible responses indicate a pass or fail status.

- Pass: The system provides an ACLI prompt.
- Fail: The system prompts you for an IP address.

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

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

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

Hardware and software compatibility

This section provides hardware and software compatibility information.

XFP, SFP and SFP+ Transceiver Compatibility

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

Table 8: XFP and SFP transceiver compatibility

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

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

Supported XFPs, SFPs and SFP+s	Description	Minimum software version	Part Number
1000BaseCWDM DDI SFP	1570nm LC connector, up to 40km	5.4.0	AA1419058-E6
1000BaseCWDM DDI SFP	1590nm LC connector, up to 40km	5.4.0	AA1419059-E6
1000BaseCWDM DDI SFP	1610nm LC connector, up to 40km	5.4.0	AA1419060-E6
1000BaseCWDM DDI SFP	1470nm LC connector, up to 70km	5.4.0	AA1419061-E6
1000BaseCWDM DDI SFP	1490nm LC connector, up to 70km	5.4.0	AA1419062-E6
1000BaseCWDM DDI SFP	1510nm LC connector, up to 70km	5.4.0	AA1419063-E6
1000BaseCWDM DDI SFP	1530nm LC connector, up to 70km	5.4.0	AA1419064-E6
1000BaseCWDM DDI SFP	1550nm LC connector, up to 70km	5.4.0	AA1419065-E6
1000BaseCWDM DDI SFP	1570nm LC connector, up to 70km	5.4.0	AA1419066-E6
1000BaseCWDM DDI SFP	1590nm LC connector, up to 70km	5.4.0	AA1419067-E6
1000BaseCWDM DDI SFP	1610nm LC connector, up to 70km	5.4.0	AA1419068-E6
1000BASE-BX bidirectional SFP	1310 nm, single fiber LC (Must be paired with AA1419070-E5)	5.2.0	AA1419069-E5
1000BASE-BX bidirectional SFP	1490 nm, single fiber LC (Must be paired with AA1419069-E5)	5.2.0	AA1419070-E5
1000Base DDI SFP	1550nm LC connector, 120 km	5.4.0	AA1419071-E6
100BASE-FX SFP	1310 nm LC connector	5.0.0	AA1419074-E6
100BASE-LX SFP	100Base-LX SFP, 1310nm, 10km, LC connector	5.6.0	AA1419081-E6
100BASE-BX SFP	100Base-BX10-U SFP Bidirectional upstream 1310nm TX 10km SFP (Must be deployed	5.6.0	AA1419082-E6

Supported XFPs, SFPs and SFP+s	Description	Minimum software version	Part Number
	with AA1419083-E6 or similar 100Base-BX).		
100BASE-BX SFP	100Base-BX10-D SFP Bidirectional upstream 1530nm TX 10km (Must be deployed with AA1419082-E6 or similar 100Base-BX).	5.6.0	AA1419083-E6
100BASE-ZX SFP	100Base-ZX, 1550nm 70-80km SFP	5.6.0	AA1419084-E6
T1 SFP	1.544 Mbps Fast Ethernet to T1 remote bridge, RJ-48C	5.1.0	AA1419075-E6
1000BASE-BX SFP	1310nm LC connector, up to 40km (Must be paired with AA1419077-E6)	5.3.0	AA1419076-E6
1000BASE-BX SFP	1490nm LC connector, up to 40km (Must be paired with AA1419076-E6)	5.3.0	AA1419077-E6
10 Gigabit Ethernet XFP Transceivers			
10GBASE-LR/LW XFP	1-port 1310 nm SMF, LC connector	5.2.0	AA1403001-E5
10GBASE-SR XFP	1-port 850 nm MMF, LC connector	5.1.0	AA1403005-E5
10GBASE-ZR/ZW XFP	1550 nm SMF LC connector	5.1.0	AA1403006-E5
10GBASE-LRM XFP	1310 nm, up to 220 m over MMF, DDI	5.2.0	AA1403007-E6
10 Gigabit Ethernet SFP+ Transceivers			
10GBASE-LR SFP+	1-Port 10 Gigabit-LR SFP+ (LC) Single mode up to 10 km	5.6.0	AA1403011-E6
10GBASE-ER SFP+	1-Port 10 Gigabit-ER SFP+ (LC) Single mode up to 40 km	5.6.0	AA1403013-E6

Supported XFPs, SFPs and SFP+s	Description	Minimum software version	Part Number
10GBASE-SR SFP+	1-Port 10 Gigabit-SR SFP+ (LC) Multi-mode fibre up to 300 m	5.6.0	AA1403015-E6
10GBASE-LRM SFP+	1-Port 10 Gigabit-LRM SFP+ (LC) Multi-mode fibre up to 220 m	5.6.0	AA1403017-E6
10GDAC-10M SFP+	SFP+ direct attach cable 10 m	5.6.0	AA1403018-E6
10GDAC-3M SFP+	SFP+ direct attach cable 3 m	5.6.0	AA1403019-E6
10GDAC-5M SFP+	SFP+ direct attach cable 5 m	5.6.0	AA1403020-E6

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

Supported standards, RFCs and MIBs

The following sections list the standards, RFCs and MIBs supported in Release 5.7.

Standards

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

- IEEE 802.1 (Port VLAN, Port & Protocol VLANs, VLAN Name, Protocol Entity)
- IEEE 802.1AB (Link Layer Discovery Protocol)
- IEEE 802.1aq (Shortest Path Bridging)
- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1s (Multiple Spanning Trees)
- IEEE 802.1v (VLAN Classification by Protocol and Port)

- IEEE 802.1w (Rapid Reconfiguration of Spanning Tree)
- IEEE 802.1X (EAPOL)
- 802.1X-2004 (Port Based Network Access Control)
- IEEE 802.3 (Ethernet)
- IEEE 802.3ab (1000BASE-T)
- IEEE 802.3ab (Gigabit Ethernet over Copper)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3ae (10Gb/s Ethernet)
- IEEE 802.3ae (10GBASE-LR/SR/LM)
- IEEE 802.3af (Power over Ethernet)
- IEEE 802.3at (Power over Ethernet)
- IEEE 802.3u (100BASE-FX)
- IEEE 802.3u (100BASE-TX)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (1000BASE-SX)
- IEEE 802.3z (1000BASE-x)
- IEEE 802.3z (Gigabit Ethernet over Fiber-Optic)
- IEEE P802.3ak (10GBASE-CX4)

RFCs and MIBs

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

- RFC 768 (UDP)
- RFC 791 (IP)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 826 (ARP)
- RFC 854 (Telnet)
- RFC 894 (IP over Ethernet)
- RFC 951 (BootP)

Important notices

- RFC 1058 (RIP v1)
- RFC 1112 (IGMPv1)
- RFC 1157 (SNMP)
- RFC 1213 (MIB-II)
- RFC 1271 (RMON)
- RFC 1305 (Network Time Protocol Version 3)
- RFC 1350 (TFTP)
- RFC 1493 (Bridge MIB)
- RFC 1583 (OSPF v2)
- RFC 1757 (RMON)
- RFC 1850 (OSPF v2 MIB)
- RFC 1945 (HTTP v1.0)
- RFC 2131 (BootP/DHCP Relay Agent)
- RFC 2236 (IGMPv2)
- RFC 2328 (OSPF v2)
- RFC 2453 (RIP v2)
- RFC 2474 (Diffserv)
- RFC 2475 (Diffserv)
- RFC 2665 (Ethernet MIB)
- RFC 2674 (Q-BRIDGE-MIB)
- RFC 2715 (Interoperability Rules for Multicast Routing Protocols)
- RFC 2737 (Entity MIBv2)
- RFC 2819 (RMON MIB)
- RFC 2863 (Interfaces Group MIB)
- RFC 2865 (RADIUS)
- RFC 2866 (RADIUS Accounting)
- RFC 2933 (Internet Group Management Protocol MIB)
- RFC 3046 (DHCP Relay Agent Information Option)
- RFC 3246 (Expedited Forwarding Behavior)
- RFC 3376 (Internet Group Management Protocol, Version 3)
- RFC 3410 (SNMPv3)
- RFC 3411 (SNMP Frameworks)

- RFC 3412 (SNMP Message Processing)
- RFC 3413 (SNMPv3 Applications)
- RFC 3414 (SNMPv3 USM)
- RFC 3415 (SNMPv3 VACM)
- RFC 3569 (An Overview of Source-Specific Multicast [SSM])
- RFC 3576 (Dynamic Authorization Extensions to Remote Authentication Dial In User Service [RADIUS])
- RFC 3768 (Virtual Router Redundancy Protocol)
- RFC 3917 (IP Flow Information Export [IPFIX])
- RFC 3954 (Netflow Services Export v9)
- RFC 3993 (DHCP Subscriber-ID suboption)
- RFC 4250 (The Secure Shell [SSH] Protocol Assigned Numbers)
- RFC 4251 (The Secure Shell [SSH] Protocol Architecture)
- RFC 4252 (The Secure Shell [SSH] Authentication Protocol)
- RFC 4253 (The Secure Shell [SSH] Transport Layer Protocol) -
- RFC 4254 (The Secure Shell [SSH] Connection Protocol)
- RFC 4541 (Considerations for Internet Group Management Protocol [IGMP] and Multicast Listener Discovery [MLD] Snooping Switches)
- RFC 4604 (Using Internet Group Management Protocol Version 3 [IGMPv3])
- RFC 4673 (RADIUS Dynamic Authorization Server MIB)
- RFC 5905 (Network Time Protocol Version 4)

IPv6 specific RFCs

The following lists supported IPv6 specific RFCs:

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

- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4291 IPv6 Addressing Architecture

The following table lists partially supported IPv6 specific RFCs:

Table 9: Partially Supported IPv6 specific RFCs

Standard	Description	Compliance
RFC 2462	IPv6 Stateless Address Auto-configuration	Auto-configuration of link local addresses only
RFC 2462	Auto-configuration of link local addresses	Supports creation of link-local addresses in section 5.3, and duplicate address detection in section 5.4.
RFC 4007	Scoped Address Architecture	Supports some behavior such as source address selection when transmitting packets to a specific scope, but there is not a zone concept in the code.
RFC 4022	Management Information Base for TCP	Mostly supported.
RFC 4113	Management Information Base for UDP	Mostly supported.
RFC 4213	Transition Mechanisms for IPv6 Hosts and Routers	Supports dual stack. No support for tunneling yet.
RFC 4291	IPv6 Addressing Architecture	Supports earlier version of RFC (3513).
RFC 4293	Management Information Base for IP	Mostly supported.
RFC 4443	Internet Control Message Protocol (ICMPv6)	Supports earlier version of RFC (2463).

Chapter 4: Resolved issues

Use the information in this section to learn more about issues that have been resolved from Release 5.6 to 5.7.

Reference number	Description
wi01092145	In a large stack, the multicast traffic is sent to all clients connected to non-base or non-temporary base units after the base units reboot.
wi01004766	QoS, Traffic Profile, IP Source Guard (IPSG): When IP Source Guard is enabled on a port having QoS traffic profiles, it occupies only one QoS precedence when enabled and frees the resource when it is disabled.
wi01009381	QoS, Classifier Name Display: The <code>show qos statistics</code> command displays classifier name correctly when track statistics aggregate option is specified for a QoS rule.
wi00961795	Upgrade to 5.6, IGMP, Unknown Multicast Allow: The previously configured Unknown Multicast Allow flood addresses are retained even after upgrading to release 5.6 or later.
wi00961775	Upgrade to 5.5 or 5.6, RADIUS Password Fallback: Radius password fallback setting is retained when the switch is upgraded to Release 5.6 or later.
wi00960742	SNTP, NTP: You can configure SNTP, NTP or clock commands from a non-base unit as well as the Base Unit or Stack IP address.
wi00932268	Port Statistics: The counters are incremented correctly when a port receives oversized and bad CRC packets or undersized and bad CRC packets.
wi00961473	Multicast Traffic, Stack of Two When one stack cable between a stack of two units fail, the multicast traffic matching the rule installed by the <code>vlan igmp unknown-mcast-allowflood</code> command allows the same traffic on all ports.
wi00950703	Management IP Address, bootp-when-needed, dhcp-when-needed: You can set IP address manually without delay, when ip address source is <code>bootp-when-needed</code> or <code>dhcp-when-needed</code> .
wi00954477, wi00955665	MAC Address Table, Layer 2 FDB: The MAC addresses associated with VLAN IDs used by STGs (4001–4008) are not shown in the MAC Address table or Layer 2 Forwarding Database (FDB).
wi00958436	EDM, MAC Address Table: When 1024 static MAC entries are added under the Static FDB tab in EDM, all 1024 rows displays with the correct ports.

Resolved issues

Reference number	Description
wi00949406	ECMP, Route Display: On ECMP configuration, the <code>show ip route</code> command and <code>show ip num-routes</code> command display the total number of routes correctly.
wi00949529	EDM, SFP: When GBICs are inserted in the ports, FO icons are displayed on first units displayed in the EDM without a manual refresh.
wi00897184	ERS 4800, Port Statistics On ERS 4800 models the port statistics for <code>ifOutDiscards</code> are incremented.
wi00870638	Port Mirroring, XrxorYtx: When you configure port mirroring in <code>XrxorYtx</code> mode, the STP, LLDP and autotopology packets are captured only during the inbound and outbound traffic.
wi00930456	MAC Security, SNMP Traps: The status of the <code>s5EtrSbsMacAccessViolation</code> trap does not get affected when MAC security is enabled globally.
wi00888446	VRRP: The <code>show</code> commands display the VRRP instance or configuration information when VRRP is configured on a VLAN using the VLAN ID 50 and 4094. Also, the default VRRP parameters are displayed for both interfaces.
wi00959485	Autotopology, SONMP: The VSP 7000 switch name is displayed correctly in the autotopology table when the ERS 4000 is connected to a Virtual Service Platform 7000.
wi00909985	AUR, QoS: QoS parameters are restored correctly when AUR performs an update of a replacement unit.
wi00961451	MAC Security, s5SbsViolationPortIdx: When MAC Security is enabled and an intrusion occurs, the <code>s5SbsViolationPortIdx</code> MIB object reports the real port index.
wi00490844	IP Source Guard (IPSG), Traps: Only link down messages are logged when maximum IP entries are learnt on a MLT/LACP enabled port.
wi00928532, wi00930048	Energy Saver, PoE Savings If Energy Saver is active and the switch or stack is reset, the power is not delivered after the switch reboots and <code>sh energy-saver savings</code> display poe savings.
wi00554891	EDM: You can have multiple EDM sessions from the same client device with multiple IP interfaces.
wi00880382, wi00891087	DHCP Snooping External Save, Transition to Standalone: You can configure DHCP Snooping External Save to use a USB port while transitioning from stack to standalone using stack force mode.
wi00491178	CPU utilization: The 'last 10 minute interval' reports the correct CPU utilization which is approximately 50 to 60 %.
wi00862054	802.1AB VLAN Name TLV: Error message does not appear when the command <code>lldp tx-tlv dot1 port-protocol-vlan-id vlan-name</code> is configured on an interface.
wi00865086, wi00954114	Avaya IP Phone DHCP Option 242, 802.1AB (LLDP) Default Parameters: If you have configured Avaya IP Phones with DHCP Option 242 to specify the

Reference number	Description
	Voice VLAN (L2QVLAN), the IP Phone use the correct VLAN if the switch is using the 802.1AB (LLDP) Default Parameters.
wi01115422	In syslog, the message “NVR Memory on unit x is under 20 M Bytes” appears as informational. This message is not saved in NVRAM. The log critical log message appears when the memory is under 15 Mbytes.
wi00850033	802.1AB Integration / Power Conservation: Avaya 9600 IP Phones does not return value 1 when the switch power conservation TLV is set to zero.
wi00849008	802.1AB Integration / dot1q-framing TLV: When Avaya proprietary TLV dot1q-framing is set to auto, the IP Phone does not use untagged mode.
wi00952359	LACP, 802.3ad: When switch/stack is rebooted, the LACP trunk numbers do not change..
wi00855665	802.1AB Integration / Phone IP TLV: IP phone starts transmitting the IP configuration details like IP address, mask and gateway address after the phone is plugged into the switch even when the IP configuration is manually configured on the IP phone.
wi00862047	802.1AB Integration / Phone IP TLV: All the IP configuration details are sent in Phone IP TLV. This TLV is used by Avaya IP Phones to advertise their IP configuration information to the switch. The IP configuration detail is displayed by the switch and can be used as diagnostic information.
wi00934177	IP Phone Automatic PoE Changes: When IP Phone consumes more than 3W, POE ports are in overload state.
wi01094340	The EDM Help is displayed for the following: <ul style="list-style-type: none"> • Edit > ADAC > DAC MAC Ranges • Security > General > Http/Https • Power management > Energy Saver > Energy Saver Globals • VLAN > VLANs > Basic/Snoop/Ports • VLAN > MLT/LACP > MLT Utilization/LACP ports • IP > IGMP > Profile • Serviceability > IPFIX > Collectors • Serviceability > RMON > Alarms > Alarms • Serviceability > RMON > Control > History/Ether Stats
wi00907795	EDM, RMON Alarms: When RMON alarm is created using variable from RMON Stats, Port Editor appears and can be selected.
wi00950722	EDM, QoS, Traffic Profile Classifier: In EDM, ignoring metering info from the QoS Traffic Profile is now possible.
wi01093077	The configuration can be saved to NVRAM while sending multiple ARP request packets.

Resolved issues


Reference number	Description
wi01035799	802.1X, EAP, NEAP, RAV, Spanning Tree: The spanning tree status of the port remains unmodified when a port is moved to a different VLAN as a result of receiving a RADIUS Assigned VLANs (RAV).
wi00927762	SFTP, Download: If you specify an incorrect IP address when you download files from a SFTP server, the system displays the correct warning message.
wi00951324	DHCP Snooping External Save, Replacing Base Unit: If you replace the Base Unit (BU) in a stack, the filename used for DHCP Snooping External Save remains valid.
wi00944065	EDM, 802.1AB (LLDP) dot1: When displaying 802.1AB (LLDP) 802.1 parameters in EDM, all dot1 lldp parameters can be displayed, including Local Protocol Vlan and Local Vlan Name information.
wi01046091	802.1X, NEAP, Multi-VLAN, Fail_Open Continuity Mode: When a switch change the operational mode from standalone to stack, if the switch is configured to use NEAP RADIUS Server and Multi-VLAN is disabled on the port, EAP clients remain authenticated during the change of operational mode.
n./a.	The syntax of the flowcontrol command is corrected to support only asymmetric, auto and disable as parameters. The parameter symmetric is no longer supported, due to hardware limitations.

Chapter 5: Known Issues and Limitations

Use the information in this section to learn more about known issues and limitations from Release 5.6 to 5.7. Where appropriate, use workarounds provided for the known issues and limitations.

Known Issues and Limitations for Release 5.7

The following table lists known issues and limitations for Avaya Ethernet Routing Switch 4000 Series Software Release 5.7.

Reference number	Description
wi01112965 wi01113343	802.1x NEAP Not Member of VLAN: For all NEAP RADIUS clients that try to initially authenticate a port unassigned to any VLAN, only RADIUS assigned VLANs from STG1/CIST are supported.
wi01113962	MAC Security Lockout Port: The MAC Address table lists the MAC Addresses even when the mac-security lockout is enabled on non-base unit (NBU) port. Workaround: Configure mac-security lockout ports and then, configure MAC security settings.
wi01115661	802.1x trace support: The trace for 802.1x related activities must be used with caution in production environments. If trace is enabled, maximum number of EAPOL clients cannot be reached.
wi01113653	MAC Security Lockout Port: When ports previously configured with mac security are included in the mac security lockout list, traffic still follows the filtering policy of mac security. Workaround: Configure the mac-security lock out ports and then configure mac security settings.
wi01081726	ISIS: The ISIS CSNP-interval does not affect generating CSNP. CNSP is generated only after the adjacency is established. All other ISIS packet types such as LSP and PSNPs are generated and received on adjacent devices.  Note: ERS 4000 does not support multi-access networks with designated routers. ERS 4000 release 5.7 supports only point to point interfaces.
wi01101547	SPBM: SPBM cannot be enabled when Autosave is disabled.

Reference number	Description
wi01103905	SPBM Cloud: Addresses learned over SPBM cloud can sometimes be displayed in CAM with a delay of few seconds.
wi01078500	SPBM: Do not use multiple redundant links between two SPB devices if multiple interfaces do not belong to a MLT.
wi01081438	SPBM: On ERS4xxx platform, if multiple VLAN are mapped to same ISID, traffic is forwarded to all VLANs.
wi01081961	SPBM: COM 3.0.1 and VSN Manager, which is the feature/component of COM, do not support 4xxx platform.
wi01075348	SPBM: NNI VLAN settings are not restored after ISIS is disabled.
wi01076939	SPBM: No log message is generated when ISIS authentication mismatch occurs.
wi01082763	SPBM: SPBM instance can not be created using EDM offbox.
wi01083290	SPBM: No log message is generated when adjacency between two SPB devices fail due to b-vlan mismatch.
wi01085468	SPBM: Unknown multicast allow flood does not work on CVLAN.
wi01115016	SPBM: ISIS is disabled on Non Base Units which are removed from stack.
wi01101543	SPBM MLT/DMLT configuration from EDM/EDM offbox (COM): All MLT/DMLT members of an ISIS interface are displayed into EDM/EDM offbox as separate ISIS interfaces in addition to the original ISIS interface corresponding to the MLT/DMLT. In ACLI, only the ISIS interface corresponding to MLT/DMLT interface is displayed.
wi01101846	SFTP Enhancement for "license and DHCP Snooping external save " configuration from EDM offbox: Response timeouts may appear in EDM when copying the license file from the SFTP server. It is recommended to use a 20 seconds timeout for the EDM offbox (COM), to avoid EDM response timeouts. Workaround: Use ACLI to copy the license file.
wi01120630	Fail Open VLAN: After defaulting the RADIUS server IP address, EAP clients might remain authenticated. Defaulting the RADIUS server IP address should be avoided when EAP/NEAP clients are assigned into Fail Open VLAN.
wi01124666	SFTP Enhancement for "license and DHCP Snooping external save " configuration from EDM offbox: Response timeouts may appear in EDM when performing SFTP-related configurations. Workaround: It is recommended to use a 20 seconds timeout for the EDM offbox (COM).
wi01127487	EDM: Some EDM tabs may be not accessible from Internet Explorer 9 and Internet Explorer 10.

Reference number	Description
	Workaround: Use the compatibility mode view in Internet Explorer versions 9 and 10 to correctly display EDM.
wi01129281	USB: The USB stick may be not recognized after hardware or software reset. Workaround: Remove and reinsert the USB stick in the USB port to make it accessible. In some cases, a reset may be needed.
wi01130870	EAP+SPBM: EAP/NEAP configuration is not supported on an SPBM enabled switch/stack.
wi01132847	SPBM: MAC Security DA filtering is not supported on SPBM CVLAN ports.
wi01133518	SPBM: When the management VLAN is configured as CVLAN, the show arp-table command does not display the MAC-IP address ARP entry of the default gateway. The ARP entry is learned and used by the switch or stack, even if it is not displayed.
wi01133635	AUR: When autosave is set to disabled, the command show stack auto-unit-replacement may sometimes display that the units are not ready for replacement. This is only a display issue; the functionality is not affected as long as you use the copy config nvram command.
wi01133641	MAC Security and SPBM : Configuring MAC Security on the NNI ports is not supported. You can configure MAC Security on the CVLAN ports. The intent of the MAC Security feature on SPBM is to be configured on the edge ports, which in SPBM scenarios are the CVLAN ports.
wi01114629	SPBM: Response timeouts may appear when using the show mac-address-table command or SPBM-related commands immediately after switch reset. It is not advisable to issue SPBM related commands or show mac-address-table command until reboot is fully complete. Workaround: Wait 4 minutes after the units have joined the stack.
wi01075599	SPBM and port mirroring: Port mirroring is not supported on the NNI ports.
wi01102653	SPBM: IPv6 management is not supported on the management ISID.
wi01119064	SPBM and DHCP Snooping/Dynamic ARP Inspection/IP Source guard: DHCP Snooping, Dynamic ARP Inspection and IP Source guard are not supported on CVLAN.
wi01133906	SLA Mon: RTP timers are displayed in EDM in microseconds instead of milliseconds.

Reference number	Description
wi01134550	RADIUS: After changing the RADIUS password in EDM, if you open a new EDM session in a different browser, an error message may appear in the second browser when trying to connect to EDM.
wi01135697	Change RADIUS password: When you set on the RADIUS server the option to disable password change for a user and you try to change on switch the password for this user, no error message is returned from a telnet/SSH session.

Known Issues and Limitations for Releases Prior to Release 5.7

The following section lists known issues and limitations in Avaya Ethernet Routing Switch 4000 Series software which are present in Release 5.7 and are also known to be present in older releases of the software.

Table 10: Known issues and limitations

Reference number	Description
wi01046652	802.1X, EAP, NEAP, RAV, Different Spanning Tree Group: When the RADIUS Assigned VLAN (RAV) for a port is in a different Spanning Tree Group to the previous VLAN assigned to the port, the RAV will not be applied. Workaround: It is recommended to use same Spanning Tree Group for all EAP related VLANs: Guest, FailOpen, EAP voice vlan, initial VLAN and RADIUS Assigned VLAN (RAV).
wi01048962	802.1X, Fail_Open Continuity Mode: You can configure Fail_Open Continuity Mode when the Fail_Open VLAN is disabled. Workaround: It is recommended to enable Fail_Open Continuity Mode only when Fail Open VLAN is enabled.
wi01042215	802.1X, MHSA, Multi-VLAN: If you attempt to configure Multi-VLAN when MHSA is also configured on the switch, the show command "show eapol multihost status" may take a long time to display output. Workaround: Customers are advised that Multi-VLAN operation should not be configured in conjunction with MHSA.
wi01048958	802.1X, NEAP, Multi-VLAN, Fail_Open Continuity Mode: NEAP clients may incorrectly remain authenticated after the re-authentication-period expires if the switch is setup to use NEAP RADIUS Server and Multi-VLAN is disabled on the port.

Reference number	Description
	Workaround: It is recommended to enable Multi-VLAN if Fail Open Continuity Mode is enabled and different Radius Servers are configured.
wi01047064	802.1X, User Based Policies, EPM: User Based Policies (UBP) must be defined locally on the switch/stack, as this implementation does not support the dynamic download of policies from Enterprise Policy Manager (EPM).
wi01060151	802.1X, User Based Policies, EDM: EDM does not provide the ability to set User Based Policies or User Based Policies for NEAP with this release. Workaround: The CLI can be used to configure these settings.
wi01035352	802.1X, User Based Policies, Filter on MAC, MHSA: If the switch port is setup for MHSA, a NEAP client authenticated after EAP device will not have the User Based Policies (UBP) filter on MAC applied to the port.
wi01037828	802.1X, User Based Policy, Change Security Level: If you change the User Based Policy (UBP) security level from high to low while clients are authorised, the high security filter will remain in place until clients are reauthorized. Workaround: To enable connected users policy to be updated, set the port to reauthorize after changing UBP security mode to low.
wi01048480	EAP, Unable to Change Port Authorization State: In a situation where all QoS precedences are used on the switch, it may be impossible to change the EAP port authorisation status from auto to unauthorized. Workaround: Change EAP port state from auto to authorized and then to unauthorized.
wi01025961	ERS4000, QoS, IP Element & Source MAC: When configuring qos ip-element Layer4 in combination with Source MAC address, you now need to specify an Ethernet type on the ERS 4500 platform.
wi01003809	802.1X/EAP, Syslog: The following error message may be incorrectly generated for EAP "EAP Error Radius - ifIndex not found port 0".
wi00978985	ASCII Script Table: A General failure message may occur when configuring an ASCII script entry with filename of greater than 30 characters. Workaround: Switch operation is otherwise not affected, specify filename of 30 characters or less when using ASCII script table.
wi00987130	EAP Trace: Trace configurations are dynamic and not saved across switch resets. Thus if you have Trace enabled in a stack and you reset one of the units within the stack, then after reset, the unit will no longer be performing trace function. Workaround: Reconfigure trace level setting after the unit is reset.
wi00989636	ERS 4500-PWR+, 4800, 4800-PWR+, Minimum Software Revision: The minimum software revision for 4500-PWR+, 4800, 4800-PWR+

Reference number	Description
	with hardware revision less than 10 is 5.6.0. The minimum software revision for 4500-PWR+, 4800, 4800-PWR+ with hardware revision 10 or later is 5.6.1. Warning: Attempting to downgrade the software to release 5.6.0 or earlier on an Ethernet Routing Switch 4500-PWR+ or 4800 (hardware revision 10 or later) will render the unit inoperable.
wi01000089	MAC Filtering, Maximum VLANs: If a configuration consisting of multiple MAC DA filter entries per VLAN with maximum number of VLANs, it is possible that the MAC FDB may be filled resulting in no space for additional MAC entries. Workaround: Ensure that the number of MAC DA filter entries multiplied by the number of VLAN configured on switch/stack is less than 8,192 entries.
wi01002073	NTP, Statistics: When NTP authentication is enabled, NTP statistics are incorrectly displayed.
wi01009029	Protocol VLAN, Tagged Ports, Changed Operation: In previous software release, if the ingress port was tagged, classification would be based on the PVID and not on the ingress packets Ethertype. The operation for Protocol VLANs has been updated to operate correctly for tagged port, such that VLAN membership will be determined first by the Ethertype on tagged ports.
wi00978033	Running Configuration, Shared-ports: The shared port commands are not output by the show running-config command or in the ASCII configuration.
wi00980989	Shared-ports, Speed/Duplex: Setting the speed/duplex parameter on a port with shared-port force is not supported.
wi00995946	Software Downgrade, Configuration Reset: When downgrading 5.6.1 image to 5.4 or earlier, both configuration NVRAM blocks will be defaulted. This is operation. Workaround: If the configuration is required on downgrade, the customer should save the configuration to ASCII and then restore this once the downgrade to 5.4. or earlier software has been completed.
wi01005690	SSH client, SNMP: If querying the switch SSH Client parameters via SNMP, the value returned by rcSshcGlobalRsaAuthentication is incorrect, you should use the SNMP object rcSshcGlobalRsaAuthentication.
wi00991539	USB: The Ethernet Routing Switch 4000 does not support USB sticks/drives formatted as NTFS. Workaround: Use USB sticks/drives formatted as FAT32 or FAT.
wi00897222	802.1AB (LLDP): If displaying the status for LLDP dot1 transmission flags in a stack which have 1024 VLANs configured, this will take considerably longer if you use the console port of a Non-Base Unit in the stack. Workaround: Avaya recommends that you perform all

Reference number	Description
	configuration and display using the console port on the Base Unit of a stack.
wi00887780	Brouter Ports: When you create brouter ports, if the maximum number of IP interfaces is reached, the following message will be displayed in CLI: %Maximum IP interfaces are already configured. In this case the system will not create the brouter port, however the port may be removed from the initial VLAN if VLAN configcontrol is set to automatic and that port will then be without VLAN membership. Workaround: To reactivate the port, add the port to the desired VLAN and re-enable STP participation for that port as appropriate.
wi00888620	Brouter Ports: Avaya recommends that you do not renumber units if brouter ports are used. This may result in routes being improperly deactivated and in loss of connectivity. Workaround: If it is necessary to renumber the stack, you should remove brouter ports, renumber the stack and then recreate brouter ports.
wi00944306	Brouter Port, MSTP: If you attempt to configure a brouter port on a port which is assigned to a VLAN configured in MSTI when running in MSTP mode, then the operation will not be applied. Workaround: If using MSTP mode, move the port to a VLAN which is a member of CIST then perform the brouter port assignment.
wi00949343	Brouter Port, STP: By design, STP participation is disabled when a brouter port is configured. If you then delete the brouter port, STP participation remains disabled on that port. Workaround: Re-enable spanning tree on the port if required after a brouter port instance is deleted.
wi00946493	DHCP Snooping Option 82: When DHCP Snooping is configured with Option 82 support and both the DHCP server (trusted port) and the DHCP client are on the base unit of a stack, then the option 82 information will not be added to the DHCP release packet or the DHCP unicast requests that the client generates. Workaround: Locate the DHCP server or trusted uplink ports on a port which is not on the base unit.
wi00939421	EDM, IP Phone Automatic PoE Changes: When IP Phone Automatic PoE Changes is enabled, the dynamic power limit or dynamic power priority is not displayed in EDM. Workaround: Use CLI to query PoE priority and limits when IP Phone Automatic PoE is configured.
wi00928161	EDM, PoE Status: In EDM PoE ports may display an incorrect status of otherFault instead of Deny Low Priority. Workaround: Use CLI to display the correct PoE status information
wi00939773	EDM, SFTP: If you use SFTP with password authentication enabled and you do not configure a password, no warning message will be generated by EDM and the SFTP operation will fail. Workaround:

Reference number	Description
	Ensure that you configure a password in EDM for SFTP if the SFTP authentication type is set to password.
wi00896456	<p>ERS 4800, 4500-PWR+: When you add an ERS 4800 or 4500-PWR+ unit to an existing stack, that stack must be running 5.6.0 or later release software. If the stack is running an earlier software release, the switch will not be allowed to join the stack as the software on these new models cannot be downgraded to releases prior to 5.6.0.</p> <p>Workaround: First upgrade the existing stack to the 5.6.0 or later software. Then add the ERS 4800 or 4500-PWR+ unit to the stack. Alternatively you could add the ERS 4800 or 4500-PWR+ unit as the new base unit to the stack; remembering only one unit in the stack can have the Base Unit switch set to on.</p>
wi00960581	<p>ERS 4800, RADIUS Management Logging: When a telnet connection is made to ERS 4800 switch operating in standalone mode, the RADIUS accounting packets sent by the switch will have the NAS-Type-Port attribute incorrectly set to Async rather than Ethernet.</p>
wi00928249, wi00928260	<p>ERS 4800, Stack Statistics: On ERS 4800 models the multicast or broadcast packet statistics are not incremented for the show stack port-statistics command output.</p>
wi00945097	<p>ERS 4800, TDR: When performing the TDR function on an ERS 4800 switch, the switch will incorrectly report swapped pairs for a straight through cable.</p>
wi00945147	<p>ERS 4800, TDR: When performing the TDR function on an ERS 4800 switch, if the switch is connected to an ERS 4500, then the switch will incorrectly report that pairs 1 and 4 are inverted.</p>
wi00936995	<p>IGMPv3: If the size of the IGMPv3 membership report is greater than 1600 bytes, the membership report will not be processed by the switch. IGMPv3 membership reports may contain join requests for multiple groups in one request. Workaround: Limit the maximum number of multicast groups per join request to less than 195 groups.</p>
wi00959759	<p>IGMPv3, Maximum Entries : The maximum number of IGMP groups learned by IGMP Snooping on the switch is 512. However, this depends on the hardware table usage. With IGMPv1/v2 there is a direct correlation between the number of groups and entries. IGMPv3 on the other hand may use more than one hardware entry per group. An IGMPv3 group with N source addresses will typically consume N +1 hardware entries. As an example an IGMPv3 group with 2 specified source will use 3 hardware entries.</p>
wi00861551	<p>IGMP, Mrouter ports: With this release IGMPv3 support has been added to the ERS 4000 product. Multicast Router (Mrouter) ports should now be configured under the ip igmp context. Following are some example ACLI commands:</p>

Reference number	Description
	<pre>ERS4000 (config)# interface vlan 1 ERS4000 (config-if)# ip igmp router 1/4 ERS4000 # show ip igmp snooping</pre>
wi00894579	<p>IGMP, Multicast Flood, OSPF: If you configure IGMP Snooping with the unknown multicast no flood option, the system drops control traffic for protocols that use multicasting (example, OSPF). Workaround: Configure unknown multicast allow flood specifically for the required multicast group.</p>
wi00934434	<p>IP Phone Automatic PoE Changes, Energy Saver: If Energy Saver has been configured for PoE power savings mode, then it will not take into account the dynamic PoE priority of a port which is allocated through the IP Phone Automatic PoE function. Thus if the underlying static PoE priority is low and even though the IP Phone Automatic PoE has set a port to high or critical PoE priority, energy saver will power down the port if poe-saver is enabled when energy saver activates. Workaround: Avaya recommends not to use poe-savings mode in combination with IP Phone Automatic PoE changes with this release.</p>
wi00929526	<p>IP Routing, Route Summary Display: When performing the show ip route summary command, the number of connected routes is incorrectly displayed as 0. Workaround: Use the command show ip route and if necessary perform a count of the directly connected routes.</p>
wi00894103	<p>NTP: You can enable NTP without configuring an NTP server, which will result in no time synchronization. Workaround: You should configure at least one NTP server for synchronization to occur.</p>
wi00895539	<p>NTP, IPv6: NTP does not support the configuration of servers using IPv6 addressing with this release.</p>
wi00934809	<p>MAC Address Table, Layer 2 FDB: With the introduction of new features such as static MAC addresses with this release, the MAC addresses of each of the units in the stack will now be shown in the MAC Address table or Layer 2 Forwarding Database (FDB). This is an expected operation and no action is required on your part.</p>
wi00962297	<p>PoE+ Firmware: In some cases it may be necessary to upgrade the PoE+ firmware on PWR+ models. In some cases if you attempt to perform a PoE+ firmware update on a stack of 8 units, the update may fail. The download will always succeed if there are 7 or less PWR+ units in a stack. Workaround: Reset the stack and attempt to reload the PoE+ firmware or remove one unit from the stack and re-download the PoE+ firmware.</p>
wi00933497	<p>Port Mirroring, Ingress & Egress Mirroring: When you use port mirroring, if a packet is both ingress and egress mirrored, two copies of the packet will be sent to the MTP ports. If the egress port is</p>

Reference number	Description
	operating in tagged mode, then one copy of the packet will be untagged and another copy of the packet tagged from the egress port. This is expected operation.
wi00955218	Port Mirroring, XrxYtx, IP Routing: When performing port mirroring in XrxYtx mode on an ERS 4500 switch, traffic which is to be routed will not be mirrored; this is a hardware limitation. When performing port mirroring in XrxYtx mode on an ERS 4800 switch, traffic which is to be routed will be correctly mirrored to the mirror to port.
wi00950622	QoS, Queue Shaping: If queue shaping min rate is configured on the highest queue number, then in an oversubscription scenario this rate may not be fully respected if it exceeds 98% from egress bandwidth.
wi00958103	QoS, Strict Priority, WRR Algorithm: The ERS 4800 will process traffic differently to ERS 4500 switches when egress queues are congested. On an ERS 4800 switch, during periods of congestion, low drop precedence traffic will be buffered, while high drop precedence traffic could be dropped if there is insufficient egress buffers available
wi00939391, wi00939393	Shared Port, SFP: New shared port functionality using the shared-port auto-select command may not work correctly on models other than the 4526GTX, 4526GTX-PWR, 4548GT and 4548GT-PWR.
wi00959035	SFP, Display: If AA14190040 or AA1419029 CWDM SFPs with the vendor ID of OCP are installed in the switch, a show interfaces or show gbic-info will incorrectly display these devices as operating at 100Mbps instead of 1Gbps.
wi00859047	SSH: The CLI command show ssh download-auth-key does not display the last transfer result when you download the key from USB. Workaround: If the download of the SSH key was successful, then when you display the ssh or sshc status you will see the key has been loaded by the switch. Alternatively loading the SSH key from a TFTP server will display the correct result.
wi00959582	SSH, DSA/RSA Key Length: When you upload the DSA/RSA key to a TFTP server or USB device from a switch/stack you can generate a filename with up to 128 characters. When you attempt to download the DSA/RSA keys, the switch supports a maximum of only 30 character filenames. Workaround: Avaya recommends you use filenames with a maximum of 30 characters for DSA/RSA keys.
wi00891090	SSH Client, Break Sequence, Syslog: When you use the SSH client from the switch or stack, if you terminate a server connection with the "~." break sequence, the system does not generate a SSH disconnected syslog message.
wi00894057	Voice VLAN, 802.1AB (LLDP) : When you can create a LLDP MED network policy there is no check performed to ensure that the VLAN type is set to Voice. Workaround: Ensure that you configure the VLAN

Reference number	Description
	appropriately as a Voice VLAN before setting the LLDP MED network policy.
wi00893827	Voice VLAN, ADAC, EAP: Avaya recommends you do not use the same VLAN ID for ADAC Voice VLAN and EAP Voice VLAN.
wi00930645	Voice VLAN, 802.1AB (LLDP) MED Policy: When you configure a VLAN as type Voice, you will still need to explicitly configure 802.1AB (LLDP) MED Network policy to advertise that VLAN via LLDP to end devices.
wi00868382, wi00554875	802.1AB / LLDP Default Parameters, ADAC: In Software Release 5.5, 5.6 and later with the introduction of 802.1AB default parameters a default LLDP MED policy is configured on all ports. The default values for that policy are as follows: application type = voice, tagging = untagged, DSCP = 46 and VLAN priority = 6, VLAN id= 0. If ADAC is configured on that port and an IP Phone is detected, the dynamic LLDP MED policy will not be installed, resulting in the IP phone not receiving the correct VLAN configuration if ADAC tagged frames is used. This happens because the default MED policy is static and overrides the dynamic policy installed by ADAC. Recommendation: If ADAC is to be used, then it is recommended that the default 802.1AB/LLDP MED policies are deleted on telephony ports and on uplink/call server ports. Use the interface command no lldp med-network-policies on telephony ports and on uplink/call server, prior to configuring ADAC on ports.
wi00863027	802.1AB Default Values: When you upgrade to 5.5 or 5.6 software, any old 802.1AB values will be maintained. The new default 802.1AB values are only applied if you reset the configuration (for example, use the boot default command).
wi00856869	802.1AB Integration / ADAC: Avaya IP Phones will perform a reset when connecting to the switch if 802.1AB Integration (use of 802.1AB TLVs) is enabled in conjunction with ADAC. Workaround: Create a manual 802.1AB-MED network policy which will then change the order in which information is supplied to the IP Phones.
wi00858022	802.1AB Integration / Avaya IP Phone: When the switch detects an Avaya IP Phone, it sends four LLDP packets (according to MedFastStartRepeatCount). With some models of Avaya IP Phone, this process is repeated 60 seconds after device detection. Workaround: None required.
wi00861373	802.1AB Integration / Call Server TLV: An IP Phone may incorrectly report the Call Server in-use IP address to the switch if different call-servers were previously configured and cached by the IP Phone. Workaround: If it is found that there is a mismatch of in-use call-server addresses cached by the IP Phone, then performing two consecutive resets of the IP Phone will clear the incorrect data from the IP Phone cache and result in correct information being returned to the switch.

Reference number	Description
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.
wi00855650	802.1AB Integration / SIP Configuration: The currently defined Avaya Proprietary TLVs, do not support the direct provisioning of SIP parameters (transport protocol, port number, domain name) from the switch to the IP Handset. Workaround: The SIP information can be supplied to the IP Phone through the configuration file server, ensure that the File Server TLV is appropriately configured.
wi00841065	802.1AB MED Network Policy: When upgrading to 5.5 or 5.6 software and the previous configuration contained no network policies, the new default network policies will be applied.
wi00841955	802.1AB MED, Auto QoS: Having a custom LLDP MED policy and enabling Auto QoS will result in the LLDP MED network policy being saved with a DSCP value of 47.
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 <code>snmp-server user</code> commented out. This is expected behavior as the associated passwords cannot be output in clear text in the ASCII generated file due to security requirements. As a result when the configuration is loaded onto a switch with default configuration, the SNMPv3 users are not recreated. Workaround: Manually recreate the SNMPv3 users after loading the ASCII configuration.
wi00491471	ADAC, EAP, Guest VLAN: If you configure both Guest VLAN (GVLAN) and ADAC untagged frames advanced mode on a port, then when a device is discovered by ADAC the port is moved from the GVLAN into the ADAC Voice VLAN. This results in lost connectivity for the GVLAN. If you disable ADAC globally, the client is removed from the ADAC Voice VLAN and placed in the initial port based VLAN with the PVID set to 1 (the default VLAN). Workaround: Avaya recommends you do not use ADAC untagged frames advanced mode in combination with EAP MHMA and Guest VLAN.
wi00932189	DHCP Snooping External Save, USB, Stack Renumbering: If you have DHCP Snooping External Save configured to save the database to a USB drive on a particular unit, then if you perform a stack renumbering the feature may incorrectly point to the USB device on the wrong unit. Workaround: If you have DHCP Snooping External Save configured to save the database to a USB drive, then after performing a stack renumbering you should re-configure DHCP Snooping External Save to use the renumbered unit in which the USB devices is located.

Reference number	Description
wi00484170	EAP, 384 ports, Intruder MAC: If you enable or activate EAP on 384 ports simultaneously, while all clients are sending large volumes of traffic, then some intruder (unauthorized) MAC addresses may not appear in the MAC address table. This applies only to intruder addresses which are blocked and not allowed to forward traffic and it is not a security or connectivity problem.
Q01981920	EAP, Fail Open VLAN: An EAP or Non-EAP client could be assigned to the Fail Open VLAN in normal operation if the VLAN name or ID returned from the RADIUS server matches the VLAN assigned for the Fail Open VLAN. Workaround: Ensure that the Fail Open VLAN name or ID that you use does not match one of the returned RADIUS VLANs.
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.
wi00484217	EAP, MHMA MultiVLAN, Guest VLAN : Switch ports are not moved into the Guest VLAN (GVLAN) if you enable the GVLAN option after EAP clients have authenticated on the port. Workaround: It is recommended that you enable Guest VLAN (global or per port option) before EAP clients are authenticated. Alternatively, you can globally disable EAP, configure GVLAN, then re-enable EAP globally.
wi00878611	EAP, NEAP, Fail Open VLAN: After the RADIUS server becomes unreachable, then reachable again, not all 384 NEAP clients may be re-authenticated in some circumstances. Workaround: After the RADIUS server becomes reachable, you can either reboot the stack or manually clear the MAC address table on the EAP enabled ports using the interface configuration command <code>clear mac-address-table interface fastEthernet <portlist></code> .
wi00491727	EAP, QoS Traffic Profiles: If you configure both QoS Traffic Profiles and EAP, in some circumstances after a switch reboot the QoS Traffic Profile may be set to a higher precedence than before the switch reboot. EAP packets could then be blocked by rules defined in the traffic profile. Workaround: To prevent EAP packet blocking in this situation, you can define a QoS policy instead of using a Traffic Profile. The same filtering capabilities are supported, but user defined policies use the same QoS precedence correctly before and after a reset.
wi00483818	EAP, RADIUS Last Assigned VLAN: When a port is configured for RADIUS Last Assigned VLAN, if the last RADIUS authentication for that port does not contain QoS priority, then the port priority will be either the one manually configured for that port or the one received for the previous authenticated client.

Reference number	Description
wi00489861	EDM, ASCII Configuration: When loading an ASCII configuration file using EDM it is recommended that the switch has minimal configuration changes from default. Otherwise existing switch/stack configuration might cause warning or error messages that force the ASCII configuration to exit with a FAIL status. Workaround: Apply ASCII configuration from EDM to a switch or stack that has a basic configuration. Alternatively, a currently-configured switch/stack can be re-configured using an ASCII configuration via CLI (console, telnet, SSH) since the system ignores warning and error messages and configuration continues until the last ASCII file line executes.
wi00906624	EDM Help, Classifier Blocks: The EDM help text for QoS Classifier Blocks incorrectly states that the eval order parameter can range from 0 to 65,535 when it should state 1 to 65,535.
wi00893619	EDM, Firefox, Ipmgr blocked: When you open EDM in Firefox on a switch/stack where the ip manager has blocked the source IP address of your browser, you will get a blank page in the Firefox browser rather than a pop-up box advising that access from your browser IP address is blocked. Workaround: Using IE will result in the appropriate pop-up box advising that access from your browser IP address is blocked.
wi00962126	EDM, Memory Utilization: The Memory utilization information which is shown in EDM may not reflect the correct values. Workaround: Use ACLI or SNMP to obtain the correct values.
wi00491403	EDM, Multiport configuration: When you use EDM to apply an operation to all ports, the system may generate a misleading error message if the change could not be applied to all ports (for example if applying a PoE setting to PoE and non-PoE ports). EDM provides only an error message indicating the first port for which it was unable to apply the configuration change.
wi00950753	EDM, QoS, Traffic Profile Committed Rate: If you configure a Traffic Profile Committed Rate in EDM, the value configured and saved by the switch will be less. Workaround: Use ACLI to configure Traffic Profile Committed Rates.
wi00876311, wi00897706	EDM, Script Busy: When connecting to EDM the following message may appear: <code>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.</code> Workaround: Check the remember option and click the continue button from the browser and the message will no longer be displayed.
wi00841212. wi00483820	EDM, TACACS+: You cannot use EDM to enable TACACS+ because the system disables Web access to the switch when you enable TACACS+ via EDM. If you used EDM to enable TACACS+ you would lose EDM access for any subsequent operations.

Reference number	Description
wi00930313	<p>EDM, USB, Binary Configuration: When saving a binary configuration file to a USB device, if you do not specify a Binary Config Filename, the following message is displayed which may be misleading: <code>No USB storage device detected.</code></p> <p>Workaround: Set the binary config filename in order to save/retrieve the configuration to/from a USB device.</p>
wi00846698	<p>EDM: EDM multiport select does not work on interfaces with SFPs/XFPs inserted. Please use per port configuration for interfaces with optics installed.</p>
Q02121888, Q02121890	<p>Energy Saver, Copper ports, RIP, OSPF: When you activate or deactivate energy saver, the link on a port briefly transitions. This transition may cause OSPF neighbor connectivity to bounce or cause relearning of RIP routes. Workaround: Avaya recommends that you disable energy saver on copper uplink ports which have OSPF adjacencies or RIP routes active. Copper ports, OSPF adjacencies—If you use copper ports for which energy saver is enabled and OSPF adjacencies are exchanged over these links, you can set the <code>ip ospf advertise-when-down enable</code> 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 <code>ip rip advertise-when-down enable</code> parameter so that RIP routes are not bounced when the link transitions. Alternative: If you use fiber ports for OSPF adjacencies or RIP route connections, energy saver will not cause a link transition.</p>
wi00900252	<p>Energy Saver: If you disable Avaya Energy Saver while it is in power saving mode on ports which are administratively set to 100Mbps, these ports will then operate at 10Mbps. Workaround: Deactivate energy saver using the <code>energy-saver deactivate</code> command in Privileged EXEC mode before disabling energy saver.</p>
wi00483987, wi00484314, wi00484346, wi00491683	<p>Energy Saver: When energy saver is activated or deactivated, the link on a port transitions briefly. This brief transition can cause some devices to reacquire connectivity, but, in most situations, end users do not notice the port transition. On the switch, the system clears the MAC address for the port and then relearns it. If EAP or NEAP is enabled, EAP authentication restarts. Workaround: Avaya recommends that you disable energy saver on copper uplink ports because activating or deactivating energy saver on copper ports triggers a link down followed rapidly by a link up event. Alternative: Use fiber ports for uplinks because energy saver does not change fiber port status when energy saver is activated or deactivated</p>
wi00931011	<p>IP Source Guard (IPSG), MLT, DMLT, LAGs: If IPSG is configured on MLT/DMLT/LAG/DLAG ports and these ports are manually shutdown, then entries may remain in the IPSG filtering table even though there are no longer any addresses associated with the port.</p>

Reference number	Description
	Workaround: Avaya recommends that if trunk ports are likely to be regularly manually shutdown and enabled, that IPSP should not be configured on trunk ports (MLTDMLT/LAGs).
Q01979384	IPv6: Due to the short, or transient, nature of TCP connections for HTTP requests it is likely that IPv6 HTTP connections may not be displayed when you use the CLI command show ipv6 tcp connections . This behavior is considered normal. Workaround: If simultaneous Web page refresh commands are issued, then a show ipv6 tcp connections command displays the active TCP connections for the Web session.
wi00489936	Jumbo Frames: As the Avaya Ethernet Routing Switch 4000 supports jumbo frames (up to 9216), the Jabber counter will always be displayed as zero (0). Workaround: You can find information about framing errors in the etherStatsCRCAAlignErrors counter.
wi00489794	Link-up during boot: During reboot or power up operations, but before the agent code loads, the switch may provide an intermittent link to devices connected to front panel ports. Regardless, no traffic switching occurs until the agent code load completes. Workaround: If uplinks are connected to fibre SFP/XFP/SFP+ devices then these devices will not provide link-up until the switch is fully operational.
wi00930449	MAC Security, MLT, DMLT, LAGs: Traffic may be incorrectly filtered if MAC security is enabled on trunk ports. Workaround: MAC security should not be configured on trunk ports (MLTDMLT/LAGs).
wi00483597	Management VLAN: When operating in Layer 3 mode, using the Management VLAN for normal routing may result in lost connectivity to the Management IP address. Workaround: If connectivity problems occur to the management IP address, clear the ARP cache.
Q02118229	MIB, EAP, MHMA MultiVLAN: If you disable the MHMA MultiVLAN option, the SNMP MIB object (bseeMultiHostStatusVid) that reports the VLAN associated with a client reports a value of either 4095 or 4096. The returned VLAN ID values of 4095 or 4096 indicate that the VLAN was not assigned to the client. This is normal, expected behavior in this scenario. Use the CLI command show eapol multihost status to confirm the VLAN ID association.
wi00848300	NEAP, IP Phone, Multi-VLAN, ADAC: If EAP Voice VLAN is used in combination with non-eap-phone option and ADAC is configured for tagged frames and EAP multi-vlan is enabled; then if EAP is disabled after IP Phone is detected and authenticated the PVID of the port is reset to the initial value instead of remaining equal to the value set by ADAC. Workaround: Perform a poe shutdown and then no poe shutdown on the IP Phone port so that the Phone is rediscovered and the PVID is set accordingly.

Reference number	Description
wi00863853	NEAP, Multiple Requests: If the switch is operating with more than 1 NEAP client per port and you issue the <code>clear mac-address-table</code> or <code>clear eapol non-eap</code> command, then the switch sends multiple consecutive access-request for the same NEAP client, during the same authentication session.
wi00900220	Port Mirroring, XrxYtx: In XrxYtx port mirroring mode broadcast traffic may not be correctly mirrored to the monitor port.
Q01977243	QoS information: Non QoS applications, such as UDP Forwarding and IP Source Guard, should be configured prior to configuration of QoS policies to avoid the potential conflict in filter precedence order which can result when the binary configuration file is reloaded. In some rare cases, when QoS precedence's are configured before non- QoS applications that use filters—for example: UDP Forwarding 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 precedence's may not be configured correctly.
Q02088900	QoS, information: The system performs bandwidth allocation for queues according to Strict Priority and WRR algorithm. When you configure shapers on queues with minimum rate, the system first queues traffic to ensure the minimum rate is achieved for all queues. The system then allocates the remaining egress bandwidth according to Strict Priority, WRR and shape maximum rate configured for each queue. In case the sum of shape minimum rates configured (queue shapers) exceeds the line rate, the minimum shape rate is assured for queue 1 and then the remaining bandwidth is distributed amongst the rest of the queues. The system uses the WRR algorithm to best assure that the minimum rates for the rest of the queues are achieved. Note: If you have ERS 4000 and ERS 5600, in the same scenario the ERS 5600 operates differently, depending on the active queue set, and may use strict priority, WRR and RR algorithms.
wi00860958	RADIUS Accounting: If RADIUS accounting is enabled and the switch/stack is reset, then the accounting messages sent to the RADIUS server will only include a <code>RADIUS Accounting Off</code> message (no <code>RADIUS Accounting Stop</code> messages will be sent for authenticated clients).
wi00878635	RADIUS, EAP Server, NEAP Server, Fail Open VLAN: While servers are unreachable and ports are in Fail_Open VLAN deletion of all of the RADIUS servers of a given type (e.g. all EAP Servers, all NEAP Servers) may result in clients not being properly re-authenticated or assigned to the appropriate RADIUS VLAN. Workaround: Do not delete all RADIUS server types when RADIUS servers are

Reference number	Description
	unreachable. Alternatively after the RADIUS servers are again reachable, manually clear the MAC address table on the EAP enabled ports using the interface configuration command clear mac-address-table interface fastEthernet <portlist> .
wi00864589	RADIUS, Interim Updates: After RADIUS accounting is disabled for a RADIUS server, interim updates will still be sent to that server, if they were previously enabled. It is recommended that you turn off interim updates also, if it is desired not to receive them.
wi00490762, wi00483513	RSTP: When operating as an RSTP root bridge and the Base Unit in a stack is reset, or the stack transitions to standalone mode, the system may not always generate the SNMP trap message indicating a change in RSTP root. Workaround: A local log message for nnRstNewRoot is always generated.
wi00484096	show running-config: When you execute the show running-config or show running-config module commands the system may take a longer time than expected to display the output. In 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
wi00496736	SNMPv3, ACG: SNMPv3 user commands (for example, snmp-server user) are commented in the text configuration file generated by the switch or stack if running the SSH version of the switch software. This happens because the associated passwords cannot be put in clear text in the generated configuration file. Please note that when the configuration is loaded the SNMPv3 users are not recreated.
wi00489857	SONMP: A change in the operation of the SONMP-based auto topology means that directly connected BayStack 450 switches report a physical auto topology change every 70 seconds to the Avaya ERS 4000 switch. You can ignore this auto topology change message where there is a direct connection from the Avaya ERS 4000 to a BayStack 450 switch.
wi00942683	Spanning Tree: When changing the STP mode from STPG to RSTP, or from MSTP to RSTP, the learning on the ports from groups other than group 1 will be set to disabled. Workaround: You will need to re-enable STP on other STP groups if so desired after re-configuration of the switch.
wi00862444	TACACS+, Layer3: In a layer 3 environment if the management VLAN is not operational (no link is up on that VLAN), the switch does not generate TACACS+ packets, therefore no authentication can be performed against the TACACS+ server. Workaround: Ensure that management VLAN is up.

Reference number	Description
wi00491296	Telnet, ASCII Config : If you configure a very short telnet timeout value and then you connect to the switch using telnet to execute the CLI command copy config, to save the ASCII configuration to USB or TFTP, the configuration file may be incomplete for large or complex stack configurations. Workaround : It is recommended to set the minimum telnet timeout value to 5 minutes.
wi00491518	VLACP : When you disable VLACP globally or on a per interface basis, the system forwards the following incorrect message to the syslog server: <code>Port X re-enabled by VLACP.</code>
wi00933290	VRRP, Management VLAN : If you create a VRRP interface on the management VLAN, the VRRP information will not be saved in the configuration file. This is operating as intended. Workaround : Avaya recommends that VRRP should not be configured on the Management VLAN of the switch/stack.
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.
wi00484079	SNMP Traps, Temporary Base Unit : If you create new SNMP Trap notification filters while the stack is operating in Temporary Base Unit (TBU) mode (that is the Base Unit has failed) then the new filters are not saved and are lost upon stack reboot. Workaround : If the stack is operating in TBU mode, reset the stack and then create the required SNMP Trap notification filters.
wi00491450	Port Mirroring, XrxYtx, XrxYtxOrYrxXtx : If you use port 1 as a mirror port in XrxYtx or port mirroring modes, then broadcast or multicast traffic mirrored to the port is doubled on the monitor port. Workaround : Use another port on the switch as the mirrored port.
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.
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.
wi00850597, wi00850936,	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

Reference number	Description
wi00850590, wi00850935	return a value of 1. Workaround: This does not result in any operational issues which require a workaround.
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.
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.
wi00483355	New VLANs created are not learned when all dot1 TLVs are already enabled on ports.
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: <ul style="list-style-type: none"> • Wait 30 seconds for the client to re-authenticate successfully • Use an alternative EAP authentication mechanism for the client
wi00897383	ERS 4800, Port Statistics On ERS 4800 models the port statistics for ipInDiscards are not incremented.

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.

Reference number	Description
4	The only IPv4 to IPv6 transition mechanism supported is dual-stack (no tunnelling).

